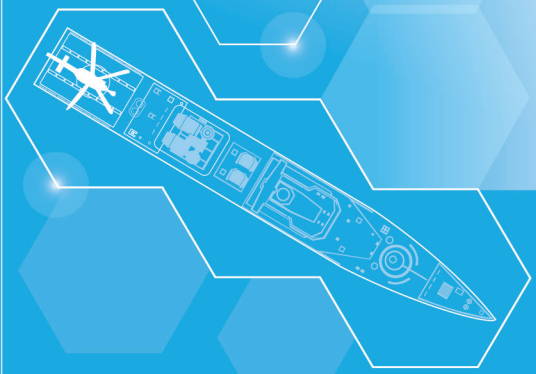


V SIMPOSIO INTERNACIONAL
DE SEGURIDAD Y DEFENSA

PERÚ 2019

Tecnología, innovación y creatividad en el campo militar

DEL 25 AL 27
DE SETIEMBRE

Por quinto año, la Marina de Guerra del Perú encargó a la Escuela Superior de Guerra Naval la tarea de organizar el V Simposio Internacional de Seguridad y Defensa.

Con el fin de satisfacer las expectativas del público asistente, se contó con expositores internacionales de larga trayectoria, a los cuales daremos mayor referencia en las páginas siguientes. Ellos compartieron sus experiencias y aportes personales para el logro de una adecuada visión de seguridad y defensa, desde una perspectiva tecnológica, ampliando nuestros horizontes en el ámbito académico a través del intercambio de conocimientos.

Agradecemos a todos los expositores por su valiosa contribución intelectual y a nuestros invitados por acompañarnos en esta larga jornada que plasmamos en la presente publicación.

CRÉDITOS

HOJA DE

DIRECTOR DE LA ESCUELA SUPERIOR DE GUERRA NAVAL
Calm. Jorge ANDALUZ Echevarría

COMITÉ EDITORIAL

Editor General:
C. de N (r) Mario VINATEA Camere

Coordinador:
Tte.1ro José RICALDE Muro

Traducción:
Tte.1ro. CC. Leslie VILLAR Jaúregui

Corrección de estilo:
Lic. Marco FERNÁNDEZ Risco

Diseño y Diagramación:
Lic. Sheylla CASTILLO Cárdenas

Transcripción:
Lic. Yvonne JARA Chauca

Colaboración:
T3. Gra. William CUADROS Rodríguez
OM.1 Geraldine ROMÁN López

Tiraje: 250 ejemplares
Reproducido por la *Escuela Superior de Guerra Naval*
Jr Saénz Peña 590
La Punta, Callao - Perú
Telef: 5190400 anexo 6123
www.esup.edu.pe

Hecho en el Depósito Legal de la Biblioteca Nacional del Perú N° 2020 - 08964
ISBN: 978 - 612 - 47941 - 1 - 7

Impreso en el Perú
Preprensa e impresión:
IAKOB INVERSIONES
RUC: 20562618008
Av. Iquitos Nro. 1481 - La Victoria
Lima. Diciembre del 2020

CONTENIDO

In Memoriam
Dr. William F. Bundy
(1946-2019)

Catedrático del U.S. Naval War College
Profesor invitado y gran colaborador de la
Escuela Superior de Guerra Naval del Perú

Calm.
Jorge
Andaluz
Echevarría
Director de la Escuela Superior de Guerra Naval

Bienvenida

Señor Almirante Fernando Cerdán Ruiz, Comandante General de la Marina, dignas autoridades, damas y caballeros aquí presentes. Sean mis primeras palabras dirigidas a dar la más cordial bienvenida a nuestro país a los representantes y expositores de Alemania, Argentina, Brasil, Bolivia, Canadá, Chile, Colombia, Ecuador, España, Estados Unidos, Guatemala, Indonesia, Israel, Italia y Suecia, deseándoles que, independientemente del motivo que nos reúne hoy, disfruten de nuestra hospitalidad, nuestro atractivo turístico y nuestra cultura. Asimismo, expreso mi más profundo agradecimiento a todos los presentes por estar aquí con nosotros para dar inicio al V Simposio Internacional de Seguridad y Defensa, evento que, con singular éxito, la Marina de Guerra del Perú, a través de la Dirección General de Educación y de la Dirección de la Escuela Superior de Guerra Naval, viene desarrollando desde el año 2014, habiéndose convertido en un espacio de reflexión, de reunión de ideas y entendimiento común en temas que se vinculan con la seguridad y defensa de nuestras naciones.

En ese sentido, más de 80 expositores y representantes de 50 países de los cinco continentes, con los que el Perú mantiene estrechas relaciones, han participado hasta la fecha en este evento. Nos enorgullece manifestarles, además, que alrededor del mundo superamos los 70 mil seguidores el año pasado, quienes en tiempo real apreciaron las exposiciones y comentarios de nuestros panelistas a través de la web.

Para la presente edición se ha contemplado como tema asociado la tecnología, innovación y creatividad en el campo militar. Para ello, contaremos con cinco bloques a desarrollar en dos días y una mañana. Los cuatro primeros bloques tratarán sobre la ciberseguridad, ciberdefensa, las construcciones navales, los sistemas de administración de combate y la innovación tecnológica, dejando para la clausura del día viernes el Sistema de Compensaciones Industriales Offset como mecanismo para el desarrollo tecnológico y el aprovechamiento de sectores distintos a la defensa, cuando en ellas se invierte. Esperamos que estos dos días y medio sean de su mayor complacencia y que generen aún más interés en los temas a tratar, fortaleciendo de esta manera nuestro común conocimiento.

Permítanme invitar al señor Almirante Fernando Cerdán Ruiz, Comandante General de la Marina, a inaugurar el V Simposio Internacional de Seguridad y Defensa.

Alm.
Fernando
Cerdán Ruiz
Comandante General de la Marina

Inauguración

Distinguidas autoridades políticas, diplomáticas, militares y civiles, señoras y señores expositores, panelistas, distinguidas damas y caballeros invitados. Constituye un honor hacer uso de la palabra en esta ceremonia inaugural del V Simposio Internacional de Seguridad y Defensa, organizado por la Escuela Superior de Guerra Naval, para expresarles, a nombre de la Marina de Guerra del Perú, la más cordial y afectuosa bienvenida a nuestro país a las distintas autoridades nacionales, extranjeras, expositores, panelistas y participantes que nos acompañan y honran con su presencia en este importante acto.

Es motivo de satisfacción para nuestra institución tener una vez más la oportunidad de ser los organizadores de este evento, el cual resaltará, en su quinta edición, el uso de la tecnología e innovación en el campo militar. Estos temas representan grandes beneficios para diversos sectores, los mismos que son considerados como necesarios por ustedes, reconocidos y distinguidos profesionales, con el fin de compartir sus invalorables experiencias y conocimientos. De este modo, consolidaremos una adecuada visión internacional en provecho de nuestras naciones.

Como parte de este simposio, disertaremos sobre temas de tendencia actual como la ciberdefensa, ciberseguridad, construcciones navales, entre otros. Un tema especial que deseo recalcar es el relacionado a las compensaciones industriales Offset, sistema que permite realizar inversiones en las grandes industrias militares a favor de los

Estados, con tecnología amigable y con visión a futuro. Esto será posible en los próximos meses, gracias a la promulgación de una Ley de offset indirecto por parte del Ministerio de Defensa.

Tengo plena seguridad en que este evento contribuirá, de manera eficaz, con la comunidad internacional en la búsqueda de nuevas alianzas y pensamientos, los mismos que nos permitirán afrontar los retos actuales y amenazas que acechan a nuestras naciones. Estoy seguro que el futuro nos tiene reservado algo mejor, siempre y cuando tengamos el valor de intentarlo y trabajar por ello. De esta manera, doy por inaugurado el V Simposio Internacional de Seguridad y Defensa.

T. J. WHITE
Nina KOLLARS
Alfred TURNER
Luis Javier PÉREZ DEL REAL

BLOQUE 1

CIBERDEFENSA y CIBERSEGURIDAD

BLOQUE

1

MODERADORES

EXPOSITORES

SESIÓN 1.1

Calm.
Enrique
Arnaéz Braschi

Para entrar en el tema, es necesario recordar que los dominios tradicionales, conocidos como tierra, mar, aire y espacio, cuentan con uno adicional: el quinto dominio, llamado también ciberespacio.

Este campo cuenta con la internet y la conectividad como parte de sus elementos, los cuales han facilitado muchos aspectos de nuestra vida a través del comercio electrónico, la banca electrónica, las comunicaciones y la cantidad de información que tenemos hoy en día al alcance de nuestras manos; en tanto, configura un hecho concreto que lo más perceptible en este campo son las redes sociales.

En tal sentido, nos resistimos a creer en distintas ficciones televisivas y cinematográficas, en las que existen riesgos y amenazas en el ciberespacio, lo que nos lleva a suponer que basta contar con un antivirus o un firewall para estar protegidos. Pensar de este modo es un error.

Para evidenciar el peligro, que comienza con información inexacta, manipuladora y hasta mal intencionada colocada en internet, les presentaré algunos ejemplos:

- Ataques a la red de bancos a nivel global.
- En julio, la prensa reportó el hackeo al Banco de Chile, mediante el cual se sustrajeron los datos de las tarjetas de crédito de los usuarios.
- En junio, también se hizo público el hackeo en los sistemas de la misma entidad bancaria. En dicha oportunidad, el robo ascendió aproximadamente a unos USD 10’000,000.
- En mayo, los medios informaron acerca del hackeo al Banco de México, hecho que significó un robo por un monto mayor a los 4’000,000 de pesos mexicanos.

Otros casos importantes son:

- En el año 2017 se registró el ataque a escala global del Ransomware WannaCry, el cual encripta la información de los ordenadores infectados y solicita un pago, a modo de rescate, para liberar la información. Quedaron afectados cerca de un cuarto de millón de ordenadores de más de 150 países y las consecuencias fueron millonarias pérdidas por la paralización de las operaciones.
- El 27 abril del 2007, se produjo el ciberataque más grande en la historia. El congreso, bancos, ministerios, la prensa y los ciudadanos de Estonia fueron el blanco de un ataque de denegación de servicios, en otras palabras, no podían emplear ninguna de sus páginas web y sus aplicativos on-line quedaron saturados y desbordados por solicitudes orquestadas. Los afectados acusaron a Rusia, pero no existen evidencias que corroboren el hecho.

Mención especial merece el hecho que, desde hace años, el grupo extremista islámico ISIS viene reclutando combatientes mediante el análisis del comportamiento y seducción, a través de juegos on-line y la búsqueda de financiamiento.

Explicada la situación y denunciadas las amenazas, deseo plantear ciertas interrogantes que serán aclaradas con las disertaciones de nuestros dos expertos: ¿cómo está conformado el ciberespacio? ¿Resulta necesario conducir operaciones en este quinto dominio?

A continuación, presentamos la opinión del Vicealmirante USN Timothy J. White, quien es Comandante de la Décima Flota de la Marina de los EEUU, y luego expondrá la Dra. Nina Kollars, docente Asociada del Departamento de Investigación Estratégica y Operacional, del Colegio de Guerra Naval de los EEUU.

sesión

1.1

Competencia por el gran poder en el siglo XXII

Valm. USN

Timothy J. White

Durante el año 2008, en mi última experiencia en el Colegio de Guerra tuve la oportunidad de leer un libro del Dr. George Friedman titulado *Los próximos 100 años*, en el cual se especulaba sobre el escenario mundial a fines de este siglo XXI. Dicha lectura hizo que reflexionase acerca de la situación del mundo en el siglo XXII y cómo llegaremos allí.

Hoy en día, los cambios ocurren de forma rápida y mañana quizás lo sean más. La raza humana está tomando mayor espacio, el mundo se vuelve cada vez más pequeño y la humanidad se conecta mediante la tecnología y con ella. Precisamente, Friedman remarcó en su obra los cambios que atestiguaron quienes vivieron en el siglo XX:

- En el año 1900, ¿quién hubiese imaginado que la era industrial, la rápida evolución del armamento y la incapacidad de la estrategia para mantener el ritmo que requería propulsarían el desarrollo de la Primera Guerra Mundial?
- Aquellos que vivieron en 1920 hasta el final de la guerra, y mucho menos los que padecieron la pandemia mundial de la gripe, ¿acaso predijeron que los mismos beligerantes, entre otros tantos, se verían sumidos en otro conflicto global?
- En 1940, ¿se pensó que el Tercer Reich, instaurado por los nazis, sería un jugador internacional dominante? Por otro lado, ¿alguno previó que la Unión Soviética de Stalin lanzaría una carrera espacial en 1957?
- En 1960, ¿era posible imaginar aquello de “un pequeño paso para el hombre, un gran salto para la humanidad”, cuando Neil Armstrong pisó la Luna o en la creación del internet?
- En 1980, ¿alguien imaginó la caída del Muro de Berlín o el final del Telón de Acero en 1990?

- En el año 2000, ¿se tuvo la capacidad de prever el atentado del 11 de septiembre y el fuerte impacto que tendría en el panorama internacional?

Ahora que se aproxima el 2020, ¿qué no estaremos imaginando?

Una parte del mundo se mueve a la velocidad del internet, sin embargo, la mayor parte del globo todavía se moviliza al ritmo del océano. Cabe preguntarnos si esto seguirá siendo así dentro de ocho décadas

Ahora bien, es necesario preguntarse también cómo *integrar la visión venidera* con la habilidad y resiliencia necesaria para *manejar la próxima sorpresa* donde sea que ocurra, incluso en el horizonte de aguas posiblemente desconocidas. Permítanme decirles que, por el momento, no tenemos una respuesta exacta sobre el futuro, pero sí alguna idea de cómo enfrentar estos desafíos tecnológicos:

- Necesitamos ser ágiles, adaptativos y colaborativos.
- Es necesario forjar alianzas, junto con coaliciones creíbles y duraderas.
- Es importante proteger la confianza de la información y promover la calidad de la misma.

En las últimas décadas, el ambiente militar ha sufrido una serie de cambios a nivel global; por ejemplo, desde la Guerra Fría hasta las misiones de paz, misiones contraterroristas y sus respectivas evoluciones, se han incorporado las redes sociales, los teléfonos inteligentes y la globalización. Por otra parte, la apertura del internet y sus vulnerabilidades juegan un papel crucial en los conflictos de poder, donde quedan comprometidas ciertas normas internacionales, que podrían amenazar la estabilidad regional.

Permítanme adicionar algunas interrogantes: ¿qué cambios encontraremos a principios del siglo XXII? ¿Cómo equilibrará cada nación las prioridades en competencia,

como la seguridad económica y nacional? ¿Seguiremos separando la seguridad nacional de la internacional? Cualquiera que sea el futuro, creemos que una base positiva será una población educada.

Para comprender mejor a dónde vamos, tomaré un momento para reflexionar sobre algunos puntos importantes. Nuestra historia compartida se remonta a 1827, cuando Estados Unidos y Perú establecieron relaciones diplomáticas. Era la época de la navegación a vela, actividad que contaba con una velocidad promedio de cinco a ocho nudos y dependía de los vientos alisios, por lo que la información y las mercancías tardaban meses en viajar por el mar. En tal sentido, la edad del vapor aumentó la velocidad tanto por tierra como en el mar, reduciendo los viajes transcontinentales y transoceánicos a solo semanas.

Por otro lado, la era de la energía nuclear revolucionó la producción eléctrica, la logística naval, la presencia marítima persistente y la disuasión. Cada edad ha visto disminuir los costos de transporte, la apertura de mercados, así como la compresión del tiempo y la distancia, pero ninguna vio la velocidad del cambio y la innovación producida en la actual era de la información.

Como hemos visto, la información está presta a convertirse en un arma poderosa, pero también ofrece cierta vulnerabilidad ante el abuso, al igual que cualquier otra revolución técnica. Por ello, hemos visto a distintos adversarios lanzar ataques cibernéticos y manipular algoritmos de redes sociales, desplegando ejércitos de *bots* y *trolls* para distorsionar, confundir y engañar al público; este es un nuevo tipo de guerra híbrida, en la que se utilizan ataques asimétricos en dominios físicos y virtuales.

Entonces, ¿cómo podremos superar el siglo XXI y enfrentar estos desafíos? Una forma específica sería mediante el forjamiento de asociaciones, en las cuales entablemos

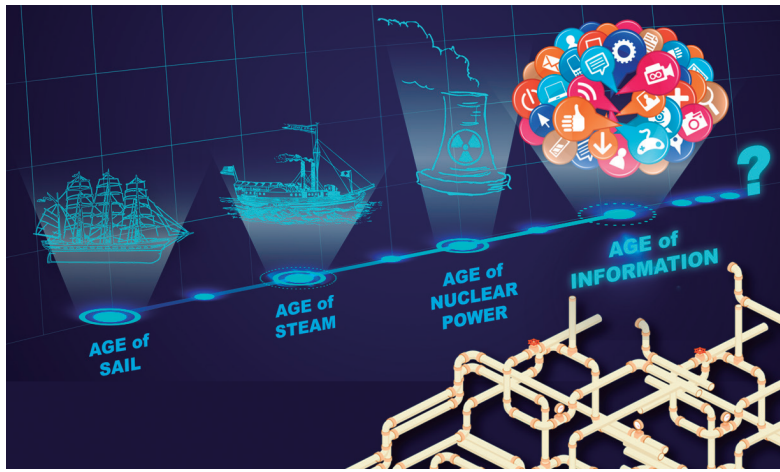


Imagen 1: en cada era se disminuyó costos durante las conexiones marítimas permitiendo la apertura de mercados.
Fuente: expuesto por el autor.

lazos de amistad con potenciales aliados. Podría decirse que esta es la mayor ventaja que tenemos en nuestro viaje hacia el próximo siglo.

Quiero resaltar que, en ese sentido, el Perú ha demostrado un admirable liderazgo regional en esta área, al establecer el llamado Grupo de Lima, que es un espacio donde los países de América Latina y el Caribe se asocian para albergar a cientos de miles de migrantes venezolanos. Nuestra disposición a prestarnos ayuda unos a otros nos brinda también la capacidad de resistir cualquier evento de cisne negro (dícese de cualquier evento de improbable ocurrencia), por incierto que este sea.

Los fuertes lazos bilaterales y multilaterales, basados en la confianza y la integridad de organizaciones gubernamentales internacionales como las Naciones Unidas y la Organización de los Estados Americanos, contribuyen enormemente a la seguridad global, haciéndola capaz de resistir cualquier desafío. Esto simboliza un importante apoyo incondicional compartido.

Asimismo, me enorgullece señalar el compromiso que mantiene el Perú con las Naciones Unidas y su membresía actual en el Consejo de Seguridad de la ONU, donde el apoyo peruano, durante los últimos 21 meses, ha sido un factor clave en el éxito de las iniciativas internacionales. Y es que Estados Unidos y Perú continúan construyendo una fuerte relación de defensa bilateral, a través de ejercicios y operaciones que mencionaré a continuación:

. UNITAS

Esta operación permitió que, durante 60 años, los buques participantes operen juntos como una fuerza de tarea multinacional combinada.

. PANAMAX

Mediante su ejecución, fuerzas de coalición practican la defensa del Canal de Panamá.

. DESI

En la que Perú tiene el liderazgo como el socio más activo, con 15 despliegues a los Estados Unidos en apoyo de los eventos de preparación de la flota.

. SIFOREX

El Perú ha sido anfitrión de esta acción durante los últimos 18 años, brindando oportunidades vitales para entrenar con submarinos peruanos.

Es nuestro deseo generar mayores oportunidades y cooperaciones entre nuestras fuerzas, para ampliar éstas y otras iniciativas en todos los ámbitos.

Los océanos son vastos y las amenazas a nuestra seguridad proliferan, ya sea por naciones adversarias u organizaciones criminales transnacionales. Esta es una de las razones por las que nuestras marinas necesitan de un trabajo colaborativo: juntos garantizaremos, de manera más efectiva, la seguridad y prosperidad de nuestros bienes comunes marítimos.

Sin embargo, es poco apreciable el alcance y la escala del cambio que está generándose. En este ecosistema tecnológico y de constante cambio, libramos una constante lucha respecto a la forma de proteger la información, el conocimiento, la propiedad intelectual, así como nuestra respectiva seguridad y soberanía nacional; si queremos atravesar el siglo XXI, debemos continuar reduciendo la propagación de la información errónea, sin que esto suponga pisotear las libertades.

Entonces, ¿cómo lidiamos con un entorno de información donde la ideología ahoga la verdad? La gente solía creer que el sol giraba alrededor de la tierra, pero los avances científicos desacreditaron dichas teorías. En la actualidad, la ciencia misma está bajo ataque. En ese sentido, ¿cómo aborda la sociedad el resurgimiento de puntos de vista extremistas aislados desde hace mucho tiempo y que recobraron vigencia gracias a las plataformas de redes sociales ? Ésta es una pregunta difícil de responder. Nuevamente, creo que la educación, el interés compartido y el diálogo abierto serán la base de una futura solución.

Las amenazas en el dominio cibernético se están expandiendo peligrosamente. En un mundo cada vez más digital y automatizado, gran parte de las funciones de control de infraestructura, comercio electrónico y gobierno se realizan en línea y están interconectadas. Dado que todo depende de los sistemas de control y automatización en red — desde la banca, el suministro de agua hasta la electricidad— es necesario reflexionar respecto a la gestión del riesgo, la forma en que se combatirán las vulnerabilidades y la protección de la infraestructura.

En el caso de los ataques ransomware, la acción consiste en secuestrar la información de corporaciones multimillonarias. De este modo, los piratas informáticos de bases de datos corporativas revelan información de identificación personal, amenazan la privacidad y la

seguridad individual, hecho que supone una cuantiosa fortuna respecto a la defensa legal de los dominios del host, sumado a los daños ocasionados en torno a la reputación y pérdida de cuota de mercado.

Es oportuno tener claro que la tecnología operativa actual no es solo de naturaleza militar. Prácticamente, todo es de doble uso e integrado, lo que significa que las operaciones en este dominio tienen efectos colaterales. Para un hombre como yo, inmerso en el mundo cibernético, la perspectiva que poseo es que la discriminación de objetivos es extremadamente desafiante. En nuestro mundo, un solo servidor de computadoras puede alojar simultáneamente un foro web extremista y un programa de prescripción hospitalaria.

Por ello, se piensa que la tecnología de la próxima generación aprovechará el *machine learning* y la inteligencia artificial. Si bien poseen una gran capacidad, este es el momento de hacer las preguntas difíciles con respecto a un mal uso potencial, al igual que otros avances tecnológicos que cambian de paradigmas predecesores y que, una vez desarrollados (como el arma nuclear), no hay quién pueda detenerlos.

Hoy en día, la conexión digital representa más de lo que se piensa; sin embargo, parece que estamos cada vez más aislados de las conexiones directas y las interacciones humanas.

Por tanto, ¿cómo entendemos las implicancias del aislamiento digital autoimpuesto? Una respuesta cercana sería a través del uso de algoritmos de redes sociales, los cuales nos conducen a burbujas protectoras y hacia cámaras de eco de nuestras propias creencias y opiniones, mientras alejamos puntos de vista competitivos. Este aislamiento disminuye la comprensión y la imaginación,

consumiendo tiempo valioso y la capacidad de atención, mientras aumenta el riesgo de reflejar imágenes de los posibles cursos de acción hacia potenciales adversarios.

El resultado obtenido parece ser una brecha cada vez mayor entre los grupos. Por ello, no debemos perder de vista las experiencias compartidas y los valores que nos unen. Una población educada y con asociaciones resilientes estará mejor equipada, cuando sea desafiada por la actividad de la zona gris adversaria.

Al igual que en la era anterior de la vela y los bienes comunes marítimos, el ciberespacio es un escenario clave en el espacio estratégico, por debajo del umbral del conflicto armado; asimismo, ofrece nuevos medios de influencia, coerción y explotación, que permiten a los adversarios obtener una ventaja estratégica sin recurrir a la agresión física.

Debemos ser conscientes que, en este preciso instante, un sinnúmero de actores está subvirtiendo, interrumpiendo y difundiendo normas internacionales de larga data, hecho que configura un robo de la propiedad intelectual a escala. Del mismo modo, a través de inversiones específicas en tecnologías emergentes, estas empresas afiliadas al gobierno u organismos estatales utilizan el comportamiento legal abierto para suplantar la ventaja del mercado en la próxima ola de desarrollo tecnológico; por último, otros fungen de agitadores geoestratégicos que emplean campañas disruptivas para socavar las fuentes de la estabilidad global, deslegitimar las instituciones democráticas, sembrar la discordia en la sociedad (a través de la manipulación del código abierto del discurso político en las redes sociales) y mellar la cohesión de la alianza.

A partir de ello, *nos vemos involucrados en un comportamiento cibernético estratégico, con la intención*

de alterar la distribución internacional general del poder. Los enfoques difieren, pero asumen al ciberespacio como una nueva ruta dentro de una gran competencia de poder, mediante la cual obtienen mayor influencia global sin involucrarse en conflictos o pisar terreno ajeno.

¿por qué es esto significativo?

Históricamente, para socavar el poder de un Estado se requería de un ataque armado abierto y violento, o bien una invasión física centrada territorialmente. Los adversarios están constantemente activos en el ciberespacio, lo que conlleva a pensar en costos acumulativos. Cada intrusión, piratería o acción técnica puede no ser estratégicamente consecuente por sí sola, pero los costos totales de capitalización son equivalentes a los recursos que requería una guerra en épocas pasadas.

Para ser precisos, la preocupación no es que la disuasión no funcioné en absoluto, sino que no detenga el creciente número de ataques por debajo del umbral del conflicto armado. Es importante mencionarles también que algunos ataques cibernéticos están siendo disuadidos, principalmente aquellos que causan muerte y destrucción, sin embargo, estas acciones no disuaden a los adversarios de las campañas en el ciberespacio, por debajo del umbral del conflicto armado.

En todo caso, los adversarios actúan deliberadamente por debajo de los umbrales aceptados internacionalmente, con el objetivo de minimizar riesgos mientras cosechan las ganancias de su comportamiento cibernético acumulativo.

Persistencia cibernética

Es necesario comprender que un viaje exitoso a través de la estabilidad del siglo XXI al XXII merece un enfoque diferente, ya que los marcos estratégicos deben alinearse con las realidades de los entornos clave. En tal sentido, es imposible imponer una estrategia.

En cuanto a las características únicas del ciberespacio, es preciso resaltar la interconexión y el contacto constante. Esta combinación induce un imperativo para la acción persistente y simboliza el desajuste con una estrategia de disuasión, basada en la restricción operativa junto a la amenaza de la fuerza.

El dominio operativo del ciberespacio requiere una estrategia de persistencia cibernética: el uso de capacidades cibernéticas debe mantener un contacto operativo para generar una ventaja táctica, operativa, estratégica, continua y capaz de producir efectos dentro, a través y desde el ciberespacio, en un momento y lugar escogido.

Este parece un espacio muy cómodo para un marino acostumbrado a operar en espacios marítimos internacionales, en cuanto a que representan actividades constantes y sostenidas que disputan y frustran persistentemente las campañas adversas del ciberespacio, antes del conflicto armado. Este es un cambio deliberado de fuerza de respuesta a una *fuerza de persistencia*.

El énfasis en la persistencia reconoce que no degradaremos a nuestros adversarios con un solo golpe y que estos no se retirarán cuando enfrenten la fricción. El énfasis en el compromiso reconoce que debemos desafiar a nuestros adversarios hoy para estar preparados mañana y en el próximo siglo. En tanto, el compromiso persistente implica habilitar y actuar.

Las fuerzas cibernéticas permiten el forjamiento de alianzas con socios interinstitucionales, internacionales y del sector privado, al compartir indicadores de amenazas, lo que proporciona un estado de advertencia y perspicacia. Asimismo, estas fuerzas actúan cuando están autorizadas por una variedad de misiones defensivas y ofensivas. Por lo tanto, para hacer algo diferente, tendremos que proceder

de forma distinta, para lograr un entendimiento común sobre la lógica de la persistencia.

Remedios compartidos probables

Para alcanzar nuestros objetivos, es necesario elaborar asociaciones operativas que abarquen todos los niveles de gobierno, el sector privado y el ámbito de nuestros aliados, con el fin de generar una conciencia situacional compartida; la colaboración oportuna, el uso compartido de accesos y el reforzamiento de capacidades son otros puntos a tomar en cuenta.

La velocidad y la agilidad serán el principal impulsor del éxito. La adaptación de viejos procesos para que sean más rápidos no será suficiente, ya que debemos inventar modelos adecuados para el cambio constante, la adaptación y la innovación. Por otro lado, tenemos al talento, aspecto necesario para desarrollar formas que propulsen el movimiento de las personas a través de la brecha público-privada a escala; la mentalidad operativa cibernética debe ser integrada en la planificación inicial y no como una ocurrencia tardía.

En este punto, ya no hablamos de la economía digital. Hoy en día nos referimos solo a la economía. Del mismo modo, no tiene sentido hablar de conflicto cibernético y guerra, pues se trata solo del segundo término. Es necesario que comprendamos algunos aspectos esenciales sobre el ciberespacio; en primer lugar, es un terreno maleable y de construcción continua, a diferencia de la soberanía, la cual es ambigua, en la que ningún acuerdo internacional sobre límites fijos bien definidos puede significar que no haya umbrales inequívocos. Esta atribución resulta ser más difícil, pero no imposible. Al igual que en los dominios físicos, en el ciberespacio hacemos reconocimiento, preparación operativa del entorno, apuntamos y maniobramos.

Por ello, es esencial pasar de una mentalidad basada en las TI, donde las redes son trabajo de los profesionales,

a una mentalidad de campaña operativa, en la que los comandantes operativos deben poseer conocimientos cibernéticos, ya que el negocio estriba en ese concepto.

En base a esta premisa, diremos que los comandantes y los encargados de tomar decisiones a nivel político no tienen que ser técnicos expertos, sino que deben poseer el suficiente conocimiento o de sus redes, para hacer las preguntas correctas y asegurarlas; y deben hacer algo que sus predecesores de la Guerra Fría asumieron: la posibilidad de operar en un entorno de información.

Finalmente, debemos entender el entorno estratégico recordando que, en el año 1900, las grandes potencias entendieron mal este concepto y terminaron envueltos en la catástrofe de 1914. La pregunta clave en torno a ello sería si estamos en esto para prevalecer o simplemente para sobrevivir. Esta interrogante ha producido un conflicto ideológico interesante, porque se desea garantizar un espacio de información abierto y gratuito, mientras nuestros adversarios se oponen a esto. En otras palabras, la polémica se resume como la *libertad de información frente al control de la misma.*

En respuesta a las amenazas actuales y al cambio de la gran competencia de poder, debemos volver constantemente a confiar en los demás, por ejemplo, en las configuraciones de una fuerza combinada, alianzas fuertes y asociaciones, intercambio de información, entrenamiento combinado, integridad, seguridad y confianza. Nuestros desafíos son comunes y requieren competencias básicas para asegurar, proteger y defender nuestros intereses en el ciberespacio.

Como antes, en nuestra historia compartida, la gran competencia de poder se ganará mediante la cooperación y los efectos acumulativos y compuestos.

La competencia del siglo XXII solo se puede ganar si asumimos a la información como columna vertebral. Este último punto representa un cambio radical en la forma en que vemos el ciberespacio y cómo nosotros, combatientes del siglo XXI, tomamos con seriedad la guerra de la información, al igual que cualquier otro elemento del poder nacional.

Espero haberles brindado algunas ideas valiosas que los lleven a la reflexión en los próximos días. A medida que contemplemos los cambios actuales y futuros en la tecnología y en el entorno de la información, podremos apreciar mejor cómo tenerlos en cuenta.

sesión

1.1

Tropezando con la actual y futura ciberseguridad de la flota: cuatro piezas fundamentales para asegurar a las armadas aliadas

Dra.
Nina Kollars

1. Mirada a la ciberseguridad de la flota futura: cuatro acertijos esenciales

Estoy segura que, para aquellos que vienen trabajando en cuestiones cibernéticas, las tres conversaciones que pueden apreciar en estos párrafos les resultarán muy interesantes, ya que enfocan partes muy diferentes de una triada cibernética: aseguramiento, defensa y respuesta.

Mis antecedentes no se parecen en lo mínimo a los de mis colegas de las marinas. Ellos son expertos en materia de guerra y de ciberguerra, sin embargo, las marinas pueden aprender de otros actores del ciberespacio, mejor dicho, aprender directamente de los hackers. Como bien saben, existen hackers buenos, conocidos como "sombreros blancos", y hackers malos o llamados "sombreros negros". Cuando nos referimos al primero de estos, solemos hacerlo bajo el término "comunidad".

Mi estudio no se basa en la táctica ni en sus técnicos, sino en las actividades de los hackers de sombrero blanco a nivel operativo y la forma en que crean nuevos conocimientos, como los difunden y la manera en que comparten informaciones relacionadas a la defensa. En mi opinión, esto es pieza clave para conseguir una seguridad cibernética efectiva en el campo militar y a nivel de las naciones.

En base a estos estudios, descubrí cuatro acertijos esenciales en los que la comunidad trabaja todos los días. Sé que no estoy aquí para decirles qué hacer, pero sí para exponerles estas interrogantes, como puntos en los que debemos reflexionar como marinas, ya que engloban el planteamiento del futuro.

En primer lugar, debemos saber que, en la mayoría de casos, hay varias personas que crean cultura cibernética. Una parte de esta es la llamada cultura MID, la cual proviene de personas, organizaciones y empresas que buscan fomentar el miedo (precisamente, MID significa miedo, incertidumbre y duda).

Las compañías de seguridad cibernética difunden MID, como una forma de generar dinero. Los piratas informáticos lo hacen de igual modo, porque los hace parecer más talentosos y, en el caso de algunos políticos maliciosos, utilizan este método porque genera una respuesta positiva por parte de la gente hacia ellos. A decir verdad, esto configura un aprovechamiento de personas que no entienden bien cuáles son los problemas tratados y sus respectivas soluciones.

Los medios de comunicación, líderes políticos, académicos y la mayoría de las personas que argumentan que todo ha cambiado a causa de la piratería están propagando el MID sin saberlo.

2. ¿Cómo vencemos al MID como naciones u organizaciones?

Particularmente, los militares están acostumbrados a considerar el peor escenario para efectos del planeamiento, sin embargo, el resto de la población es propensa a enloquecer al verse amenazada. En ese sentido, los hackers no son diferentes, pues pasan la mayor parte del tiempo soñando con formas locas e innovadoras de romper cosas, pero la mayoría toma esto como un pasatiempo.

Algunas de estas personas tienen trabajos en seguridad, característica que los diferencia de aquellos que se encuentran inmersos en actos de piratería, pues entienden que la seguridad cibernética se trata realmente de pensar en los cuatro acertijos, los cuales mencionaré a continuación:

- Averiguar cuáles son los riesgos reales.
- Descubrir cuál es la protección contra esos riesgos.
- Asociarse con otros que tienen riesgos similares.
- Equilibrar los riesgos cibernéticos.

Cuando hablo sobre el riesgo que corren los militares recibo una de dos respuestas. Cabe mencionarles que he

comenzado a pensar en esto como una especie de prueba de Rorschach, la cual consiste en proveer una imagen ambigua que podría parecerse a cualquier cosa. Lo que se cree ver suele ser un indicador de lo que se tiene en mente. Pues bien, al hablar de riesgo cibernético, o bien responden “riesgo aceptado”, o bien dicen “todos vamos a morir”. Lo importante es saber que, en el tema cibernético, no hay respuestas intermedias.

Bruce Potter, uno de mis piratas informáticos favoritos, es consultor de seguridad para agencias de inteligencia de los Estados Unidos de América, organizaciones militares y para el público en general. En ocasiones, realiza consultorías para empresas y fue precisamente por ello que un día recibió una llamada telefónica por parte de una pequeña empresa y se dio con la sorpresa de que el dueño estaba frenético. La empresa era un negocio local que tenía un sitio web y Bruce tomó la llamada por curiosidad; luego, el dueño del negocio le explicó que necesitaba protección para sus bases de datos, pues estaba seguro que la NSA (la Agencia de Seguridad Nacional de los Estados Unidos de América) iba a espiarlo, por ser ciudadano estadounidense y poseer clientes estadounidenses, para robarle los registros de sus consumidores ¿Es probable que esto ocurra? ¡Por supuesto!

En ese sentido, cabe preguntarse si es probable que la NSA robe los registros de una pequeña empresa estadounidense. Eso sería ilegal, entonces, es altamente improbable. Ahora pasemos al caso de un ejército, específicamente al contexto de las marinas de guerra.

Actualmente, los Estados Unidos de América se encuentran desarrollando una imagen detallada de los activos militares críticos y si esas instalaciones son seguras, envejecidas o vulnerables; también están identificando qué misiones son críticas y evalúan si esos activos necesitan reemplazo o movimiento.

En mi trabajo con la comisión Cyber Solarium, reflexionamos sobre la infraestructura crítica, respecto

a cuales son los servicios necesarios para mantener nuestras ciudades en funcionamiento. Les aseguro que quedarían sorprendidos con lo que hemos aprendido. Por ejemplo, en el sector financiero responden que, en muchos casos, solo necesitan la impresión de dinero; en el sector del agua responden que no tienen necesidades cibernéticas inmediatas, sino enormes requerimientos físicos; mientras que en el sector energético responden con la resiliencia y recuperación. Esto es solo el activo físico, sin embargo ¿qué pasa con las redes de datos lógicos?

En otras palabras, el segundo paso para garantizar la misión será el mapeo no solo del activo físico, sino también del activo lógico, con el fin de entender la interacción entre ambos.

Por otro lado, gracias a un trabajo de investigación, uno de mis alumnos descubrió que si bien la misión puede comprender la vulnerabilidad del activo físico, existen dificultades para entender las pertenecientes al espacio lógico y su responsabilidad. Supongamos que tenemos un puerto en algún lugar cercano al Canal de Panamá; para el desarrollo de la misión, los activos que importan son claros y de propiedad clara, pero, ¿qué pasa con los centros de datos que enlazan con ese puerto? ¿Cómo se construye y quién posee ese activo lógico?

En el proceso de los juegos de guerra y en base a mi experiencia en el Colegio de Guerra Naval, hemos descubierto una y otra vez que el nivel de secreto asignados al concepto cibernético hace que sea extremadamente difícil enseñar y aprender, ya sea en el aspecto defensivo u ofensivo. Asimismo, una pregunta constante que debe abordarse es cómo hablar de eso. Desde el lado defensivo, la pregunta gira en torno a las vulnerabilidades.

En el mundo de los hackers, las vulnerabilidades ocupan la totalidad de la discusión, por ejemplo, las políticas de divulgación de las mismas. Sin embargo, se pone el énfasis requerido en las capacidades, la falta de práctica y

la sincronización, ya que en dicho proceso se descubren los riesgos.

La asociación entre militares en el dominio físico es saludable y debe fomentarse, al igual que la interoperabilidad entre unidades, para garantizar la comprensión del mismo lenguaje y las maniobras de nuestros aliados y sus fuerzas. Sin embargo, la asociación en cibernética y redes debe hacerse con mucho más cuidado.

Desafortunadamente, muchos activos y armas funcionan en sentido opuesto cuando hablamos de cibernética, ya que la conexión entre redes significa una red propia es tan fuerte y resistente como la menos protegida. En tal forma, para minimizar riesgos y vulnerabilidades, debemos aprender y compartir continuamente nuestros datos e ideas.

Lo sorprendente de la Comandancia de Ciberdefensa de la Marina de Guerra del Perú es su enfoque colaborativo, el cual va más allá de las relaciones de Estado a Estado, respecto al desarrollo de capacidades, englobando a todos los actores y agentes potenciales en el ecosistema de la seguridad.

Al principio, en el mundo de los piratas informáticos, las acciones de aprendizaje e intercambio se realizaban de forma encubierta, lo que motivaba a los hackers a compartir sus ideas en redes confiables. Desde entonces, a medida que los gobiernos, las empresas privadas y las organizaciones se han dado cuenta de la amenaza que esto supone, el intercambio de información en todas las jerarquías ha mejorado.

Luego de compartir estas ideas, habiéndonos aproximado hacia diferentes enfoques de las formas de trabajo en el ciberespacio, planteamos la solución a los cuatro acertijos: la respuesta es encontrar el balance entre ellos.

SESIÓN 1.2

C. de N.
Luis
del Carpio Azálgara

La segunda sesión tratará respecto al tema de ciberseguridad y ciberdefensa, conceptos que, como vimos en la primera parte, se desenvuelven en un entorno complicado. Actualmente, poseemos un nivel de conexión mundial que posibilita la transmisión de información a alta velocidad y facilita nuestras vidas, el comercio, la banca, el tráfico aéreo y marítimo. Precisamente, gracias a esta interconexión se realiza este simposio, ya que todas las coordinaciones hechas para contar con la presencia de expositores internacionales y representantes de las Armadas de otros países fueron posibles gracias a esa conectividad existente en el internet.

El ciberespacio nos ofrece la facilidad de obtener información e interconectarnos no solo con computadoras, sino también con sistemas físicos. Esto brindó una gran capacidad de desarrollo, lo que devino en el proceso de la globalización, sin embargo, trajo también nuevas amenazas; cabe mencionar que estos peligros no solo atañen a los sistemas de las computadoras, sino también a las máquinas, sistemas automatizados y procesos ligados a ellos, lo que representa un alto riesgo en el ambiente cibernético y en el ámbito físico.

Esta sesión cubrirá el tema de las amenazas y la descripción del entorno, así como la forma en que deben enfrentarse los peligros en el ámbito nacional y en el dominio marítimo.

En tal sentido, el Sr. Luis Javier Perez del Real disertará respecto a cómo una nación debe organizar un centro de ciberseguridad nacional, presentando los riesgos y amenazas que un país enfrenta actualmente y cómo debe organizarse este centro para hacerles frente. Por otra parte, hará una revisión sobre la organización e interacción con los diferentes estamentos del Estado, para el forjamiento de una seguridad integral que permita el normal desarrollo de una nación.

Por otro lado, el Capitán de Navío USN (Ret) Alfred Turner presentará las implicancias del ciberespacio en las operaciones que se realizan en el ámbito marítimo. Las marinas de guerra realizan operaciones en el dominio marítimo, lo que hace necesario entender que existen amenazas que no solo influyen en las redes, sino también en dichas operaciones.

Asimismo, se presentarán conceptos y diversos análisis de las amenazas y de los recientes ataques en el ciberespacio que causaron impactos significativos en las operaciones marítimas y en la seguridad internacional. Finamente, se expondrán algunas formas de cómo hacer frente a estos retos, para mitigar sus efectos.

sesión

1.2

El Centro de Ciberseguridad Nacional: una visión práctica

Ing.
Luis Javier
Pérez del Real

En esta exposición plantearemos algunos puntos sobre la visión del Centro de Ciberseguridad Nacional, desde una perspectiva práctica de operaciones y funciones. El concepto arraigado que se tiene en cuanto a seguridad es que todo salga como se espera. En base a ello, lo que se busca en un Centro de Ciberseguridad Nacional es el éxito y para esto se debe determinar si la organización cuenta con una infraestructura crítica capaz de mantener umbrales seguros y tolerables de operación, donde no existan desviaciones en cualquier aspecto. Asimismo, revisaremos el estado del arte, los objetivos y la agenda nacional, la organización operacional de dicho centro y los retos a futuro, debido al avance tecnológico.

En la actualidad, hay un punto importante relacionado a la forma de pensar del atacante. La perspectiva empresarial es muy distinta a la que poseen las fuerzas militares y se debe tener en cuenta que hay cierto vínculo entre ambos campos. Ahora, cambiemos el tema del atacante común al adversario; cuando se habla de un adversario debemos considerar que puede ser una persona o un grupo con un objetivo definido, disponibilidad de recursos y que buscan cumplir con una agenda.

Imagen 1: motivaciones del atacante.
Fuente: expuesto por el autor.

Los adversarios pueden tener muchas cosas, pensar en otras tantas y basarse en diferentes motivaciones. Sabemos que hay naciones en donde las organizaciones de servicios y empresas son propiedad del Estado, entonces, a estas les interesa atacar otros Estados para hacerse con información de propiedad intelectual. Otras simplemente lo hacen para obtener inteligencia y tener ventaja, en cuanto a la ejecución de un ejercicio cinético de forma efectiva. Por ello, debemos analizar cómo es ese adversario: si este se anuncia o si prefiere estar en las sombras para ocultar su identidad.

Es relevante mencionar que, cuando descubrimos rápidamente quién es el atacante, se cumple lo que dicen las encuestas comerciales respecto a que un ataque dura ocho minutos. Sin embargo, dejemos las especulaciones de lado, aquí estamos frente a alguien que quiere molestarnos sin que nos demos cuenta. La historia cambia cuando empezamos a ver cosas sospechosas, ya que en ese momento ocurre lo interesante y es cuando realmente debemos poner a todo el personal disponible a investigar qué está sucediendo. En la presente exposición mencionaremos, además, cómo generar un marco sólido para ejecutar esta tarea a nivel nacional.

El proceso inicia estableciendo un pensamiento similar al del atacante: ¿qué tan focalizado es?, ¿qué tipo de activos tiene y cómo hace esto? De este modo encontraremos muchas motivaciones y la visión del adversario, por mencionar algunas características. En el caso del hacker denominado *blackhat* (atacante de sombrero negro o malicioso) tiene una agenda bien definida. En relación a ello, se cuenta con una amplia gama de tipos de adversarios, en el que podemos apreciar que muchos de ellos comparten características similares, sin embargo, podemos afirmar que se trata de gente altamente experimentada y que, en el peor de los casos, son financiadas por un Gobierno, poseen recursos ilimitados en infraestructura, tienen jefes

Imagen 2: motivaciones del atacante- visión del adversario.
Fuente: expuesto por el autor.

de proyecto y cuentan con centros de operaciones. En ese sentido, diversas campañas en países de Asia descubrieron que, cuando dejan de recibir ataques, se debe a que es día feriado en el país de los adversarios. Eso representa un indicador de compromiso que puede ayudar a identificar el origen.

Cabe mencionar que uno de los principales problemas de la ciberseguridad es la atribución, lo cual refiere la posibilidad de señalar al responsable del ataque. Es posible investigar y establecer que un ataque salió de cierto dispositivo, pero es muy difícil aseverar quién lo hizo. Por ejemplo, hay países que, una vez perpetrado su cometido, se hacen pasar por otras naciones colocando pedazos de código en otro idioma, entre otros mecanismos. Esto indica que los adversarios utilizan técnicas creativas y se han vuelto muy inteligentes con el paso del tiempo; asimismo, en diversos foros se observa que intercambian varios indicadores entre ellos, con el único fin de distraer a sus víctimas.

Es importante mencionar algunas de las características particulares de cada grupo, como las herramientas que utilizan y algunas tácticas específicas. Este tema es relevante porque no todos tienen acceso a las mismas herramientas. Cuando decimos que un adversario tiene

dinero y posee equipos de investigación, prevemos que todos los esfuerzos deben enfocarse en analizar cuál es el daño que pueden generar y la infraestructura que quieren atacar. Por otro lado, los tipos de adversarios pueden clasificarse en los que basan sus acciones en la motivación y en la habilidad. Tenemos vándalos, programadores, ladrones, criminales y espías trabajando para diferentes organizaciones. Si nos preguntamos quienes están

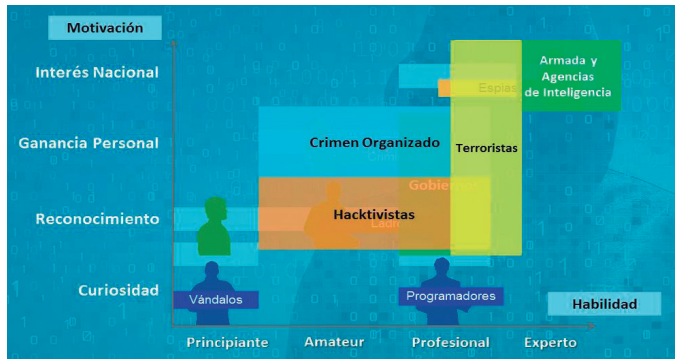


Imagen 3: Tipos de adversarios.
Fuente: expuesto por el autor.

detrás de ellos diríamos, sin lugar a dudas, que el crimen organizado.

En efecto, existen casos en los que el crimen organizado ha contratado los servicios de atacantes para realizar encargos de extremo a extremo (controlando la cadena de suministro) así como intrusiones en puertos, empresas mercantiles y gubernamentales e instituciones financieras, con el objetivo de seguir operando. Si observamos estos escenarios de forma aislada, es muy probable que no hallemos un contexto, pero, si lo analizamos desde una perspectiva nacional, obtendremos información relevante que será objeto de un estudio profundo.

Otra cosa muy distinta ocurre con el ciberterrorismo, sin embargo, su denominación no es muy clara debido

que, hasta hoy, no se tiene una definición mundialmente aceptada acerca del de terrorismo. Todos sabemos por dónde va la explicación, pero a nivel de instituciones, por ejemplo, encontraremos diferencias sustanciales entre la concepción que se tiene en La Haya, de la que se asume Washington y todas circulan, por lo general, en la misma línea . Ahora bien, ¿qué hace realmente un ciberterrorista? Quizás estemos frente a una persona que destina sus esfuerzos a hackear una fábrica de cereales, para cambiar los componentes y envenenar a la población infantil de un país, o tal vez su único objetivo sea crear caos y confusión.

Imagen 4: detrás de un adversario hay personas .
Fuente: expuesto por el autor.

Recordemos que detrás de un adversario siempre hay una persona. Esto es muy importante, ya que la tecnología que utiliza es el reflejo de la personalidad de dicho individuo y su cultura. Por ello, debemos analizar cuál es su objetivo, en cuanto a si es aleatorio o si realmente posee un patrón capaz de descubrirse a través de la investigación. En tanto, es necesario estar atentos respecto al nivel de preparación del ataque y a las tendencias; por ejemplo, si estuviésemos frente a ataques de tipo *low and slow*, será preciso apuntar que estos son muy lentos para evadir los mecanismos de detección tradicionales.

Por otro lado, un punto primordial en la gestión del centro de ciberseguridad nacional es la disciplina. Un analista no recuerda las últimas veinte alertas que revisó el día anterior, por lo que resulta muy probable que dejase de lado esta actividad, cosa que terminaría siendo perjudicial para los intereses del centro. Quizás piensen que esta premisa es demasiado drástica, pues cabe preguntarse si a diario se realizan investigaciones de actividades sospechosas o cada cierto tiempo.

Un grupo social se atribuye varias acciones, como el hecho de saber cuánta infraestructura se tiene; sabemos que hay sitios, en China particularmente, donde los proveedores de servicios de internet son conocidos por ser hostiles y por ofrecer servicios de hosting a los atacantes. Entonces, si tenemos identificada toda esta infraestructura alrededor del mundo, ¿es necesario compartir esta información con los demás? Este es un punto muy importante para conseguir un panorama general de lo que hacemos. Lo otro es determinar si estas personas tienen dinero o no, pues hay cosas que solo se ejecutan con una economía solvente, como la capacidad de tener infraestructura y herramientas nuevas.

Hace dos semanas, en el mercado negro pagaban alrededor de un millón y medio de dólares por un ataque desconocido hacia el IPhone (llamado ataque día cero, o 0-day). Ahora, la tarifa se incrementó a dos millones y medio de dólares por una vulnerabilidad día cero para Android. Como vemos, el interés de los atacantes y las organizaciones ha cambiado, lo que evidencia la existencia de adversarios con capacidades de investigación y generación de herramientas. Algunos las adquieren a través de terceros y otras simplemente utilizan herramientas disponibles en internet.

En el año 2019, en el aeropuerto de Lima resonó una alarma que sobresaltó a algunos pasajeros, sin embargo, el personal del terminal comunicó que se trataba de

pruebas realizadas en el sistema de extinción de incendios. Lo interesante es que, en este caso, una organización dio aviso de lo que venía sucediendo, pero imagínense que un día cualquiera de ustedes se encuentra en un aeropuerto en el extranjero y de pronto advierten por los parlantes que hay una bomba o que liberaron ántrax en el recinto. Créanme si les digo que eso representa la creación del pánico y el terror.

Algo similar a lo sucedido en Lima ocurrió en el aeropuerto de Vietnam en el 2016, aunque no de forma tan drástica. El ataque alteró las imágenes y pantallas del terminal aéreo, en las que se mostraba información sobre los vuelos. La motivación del hecho fue el activismo por los problemas en el mar del sur de China; los hackers cambiaron el sistema y tomaron el control de sonido del aeropuerto. Este caso es interesante, pues más de uno seguro preguntará para qué puede servir algo tan simple: pues para sembrar pánico y generar zozobra entre la gente que está ahí. Asimismo, otro de los objetivos fue la fuga de información de todos los miembros del programa de lealtad de Vietnam Airlines. Los atacantes querían demostrar algo y lo lograron muy fácilmente, tras vulnerar una infraestructura crítica como el aeropuerto.

Ahora bien, imaginemos en que pensaban los atacantes al perpetrar este acto. En primer lugar, definamos cuál es el mejor objetivo para causar mayor impacto; en palabras de los responsables, quizás dijeron <<me interesa que se den cuenta y cinco minutos después no pasó nada>>, <<lo hago en una hora pico, en un lugar donde los ojos del mundo podrán ver lo que sucede>>. Dependiendo de los objetivos, el atacante se preguntará qué tipo de sistemas tienen y cuales conectan con las pantallas de vuelos. Muchas veces, en los aeropuertos podemos ver puertos o interfaces de conexión dónde podemos dejar un dispositivo del mismo tamaño que un móvil pequeño, para infiltrarlo en la red.

Hace 20 años, un ex miembro de la NSA americana fundó una empresa. Si recuerdan la famosa Nokia 800 —una tablet pequeña que poseía Linux—, deben saber que en esta empresa se desarrolló un software que se vendió junto con la tablet por mil dólares, para que fuera comprada y entregada a una potencial víctima. Esta solución, en cuanto detectaba que el usuario estaba conectado a una red inalámbrica, recolectaba las contraseñas y atacaba todos los equipos del entorno, reportándolos a un sistema de comando y control. Esto ocurrió hace más de diez años, hoy en día, esta acción se realiza mediante cables inteligentes; si tienen un iPhone y compraron un cable que no es el original, el dispositivo muestra el mensaje de cable no certificado, ya que es posible entregar datos de control de esta forma. Si la batería de nuestro móvil está a punto de agotarse o, caso contrario, aplicamos otra técnica para que el teléfono consuma energía, nuestro objetivo quedará vacío y saldremos en busca de la recarga correspondiente. Es en ese preciso momento en el que pisamos territorio enemigo.

Lo expuesto anteriormente son ejemplos que demuestran lo que puede pasar dentro del espectro y lo que podrían hacer nuestros adversarios. Sus acciones van más allá

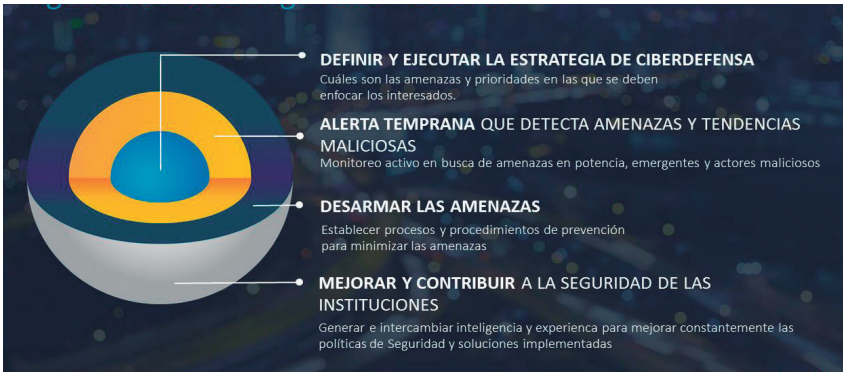


Imagen 5: Agenda de Ciberseguridad Nacional.
Fuente: Verint Systems Inc.

del desarrollo tecnológico, pues no solo fabrican cámaras pequeñas con el fin de ocultarlas, sino que definen como infiltrase en las redes de los demás y persistir en dichos canales. También se preocupan por la forma de evitar la detección, siendo relevante para ellos la capacidad de continuar infiltrados y, ante una guerra cinética, reaccionar de forma alterna.

Comentaban hace un momento casos de Ucrania y otros lugares donde se han hecho negaciones de servicio. Imagínense que están en invierno, bajo diez grados centígrados y atacan la red eléctrica o las redes de gas. Es muy probable que esto genere la muerte de muchas personas a causa del intenso frío. En base a esto, tenemos varios temas que comentar y sobre los cuales reflexionar.

La agenda de ciberseguridad nacional debe enfocarse en definir y ejecutar una estrategia de ciberdefensa, mediante la identificación de prioridades a las que se debe abocar un determinado grupo de trabajo. Otro punto es determinar cómo conseguir y emitir una alerta temprana que detecte amenazas y tendencias. Si yo sé que algo está pasando, ¿cómo puedo comunicárselo a las demás partes para que no nos afecte a todos? Tengamos en cuenta que la filosofía de la seguridad perimetral es obsoleta en la actualidad. Es importante asumir que podemos ser víctimas de un ataque en cualquier momento, lo que sugiere estar listos para reaccionar oportunamente. Imaginen que estamos a punto de caminar por un barrio peligroso, ¿cómo debo afrontar dicha travesía? Quizás sea pertinente no llevar la cartera llena de dinero o cargar poco efectivo para minimizar el daño. Lo mismo sucede en el mundo cibernético: debemos pensar en un ataque inminente y, por tanto, será necesario minimizar los impactos y la forma en que esto se pueda expandir a otras organizaciones.

Del mismo modo, hay que considerar cómo desarmar las amenazas. Sí sabemos que un ataque está en curso, ¿será necesario implementar un sistema de detección para

analizarlos o bloquearlos, para hacerles saber que han sido identificados? En cuanto a las capacidades ofensivas, si es posible investigar cómo funciona un determinado actor, puede ser muy interesante obtener todo ese conocimiento y pasárselo a mi equipo de capacidades ofensivas, para que adquieran también esas capacidades.

Será muy beneficioso, además, averiguar cómo mejoramos y contribuimos a la seguridad de las instituciones. Típicamente lo hacía el CERT (*Computer Emergency Response Team* o Centro de Respuesta a Incidentes) o las mismas universidades, que en muchas ocasiones iniciaron estos esfuerzos. Asimismo, hay CERTS nacionales que fungen como semilleros del talento y aquí es donde ingresa mi contribución sobre cómo hacer un CERT nacional, al menos para los suscriptores de infraestructura crítica de las Fuerzas Armadas. Es importante tener en cuenta cómo responder ante todo eso.

De igual modo, es de vital importancia saber qué nos puede afectar a nivel nacional. Los servidores del gobierno, la misma seguridad nacional, el espionaje, el terror, la infraestructura crítica, todo contribuye a la vulnerabilidad, ya que sabemos de antemano que los ataques pueden afectar a las empresas de energía, a las empresas petroleras, el sistema financiero, entre otras entidades; este fue el caso de México, cuyo sistema fue atacado desde el Sistema de Transferencias Interbancarias y el famoso SWIFT, supuestamente por actores hostiles que operaban en Asia. Por tanto, debemos tener una visión clara de qué está pasando, para defendernos de estas organizaciones que podrían afectar el desempeño de la agenda del país; asimismo, es necesario determinar cómo generar una continuidad de negocio y que las entidades no cedan ante un ataque. Esto conlleva a una preparación basada en la resiliencia, lo que devendrá, además, en un voto de confianza hacia los inversionistas. Si las empresas son atacadas, evidentemente las empresas públicas pierden

Imagen 6: ¿qué ve elSOC Nacional? .
Fuente: Verint Systems Inc.

valor en la bolsa, pero si una empresa internacional es atacada en su país de origen, puede perder la confianza y la matriz dejará de invertir.

Ahora, determinemos que es lo que podemos apreciar mediante el SOC nacional (*Security Operations Center* por sus siglas en inglés o Centro de operaciones de seguridad). De acuerdo a lo permitido por la legislación vigente, será posible observar el tráfico internacional que entra y sale del país. Por otro lado, es importante tener convenios de colaboración muy estrechos con las operadoras (recuerden que representan una infraestructura crítica medular, ya que a partir de ellas es posible generar ataques). En tanto, es importante saber qué acciones se llevan a cabo en el marco de los convenios, compartir esta información y habilitarlos para un óptimo reporte.

Si visualizamos el tráfico internacional, asistiremos como espectadores privilegiados de lo que entra y sale del país. A lo mejor entró un ataque a la presidencia, luego se movió hacia la Armada y, posteriormente, recayó en la Fuerza Aérea; entonces, mediante un proceso de rastreo inmediato, se determinará si esta acción responde a una campaña hostil. En otro momento, quizá veamos el tráfico nacional y detectemos a un nuevo operador que ofrece internet por 4G, el cual podría ser utilizado por los

atacantes para comprometer sitios del gobierno o atacar a las operadoras.

Las organizaciones monitoreadas son aquellas que caen debajo de ese paraguas de seguridad nacional y que pueden ser reguladas, asesoradas y protegidas hasta cierto punto, mientras que las organizaciones de terceros, básicamente, son suscriptores de servicios que podrían pedir ayuda en algún momento.

Un punto interesante, de acuerdo a los datos de los últimos años brindados por una empresa llamada Mandiant, es que, en promedio, una campaña de ataque puede durar cien días, ya que es el periodo en que se genera una brecha y se reconoce a los atacantes dentro de la estructura.

Imagen 7: extracto de un periódico sensacionalista.
Fuente: expuesto por el autor.

Dichas campañas buscan ser operaciones persistentes en cuanto al mantenimiento del acceso e involucran no solo

una organización, sino toda una cadena. En la actualidad, hackear el iPhone ya no representa una vulnerabilidad, pues existen hasta cinco vulnerabilidades encadenadas para llegar a un objetivo. Lo mismo sucede con los objetivos de seguridad nacional: sí yo sé que hay una relación de confianza entre una u otra organización, tal vez no llegaré a la que esté más protegida, sino a la de los terceros. Históricamente, así es como se ejecutaron los grandes ataques a empresas retail, operadores de telefonía, líneas aéreas, entre otras.

El análisis de las noticias de un periódico de prensa roja es semejante al panorama de inteligencia que teníamos en ciberseguridad. Yo veía unas cosas y seleccionaba lo que podría significar un ataque y lo que no. Entonces, es necesario desarrollar un enfoque mucho más asertivo, donde se pueda decir si un elemento constituye realmente una amenaza o si representa una coincidencia con algo que se le parece.

El panorama cibernético nacional debe buscar quienes son los actores maliciosos e identificar la infraestructura maliciosa dentro del país. Es conocido que en Perú tienen buenos desarrolladores de malware bancario y de *botnets*, al igual que en Brasil, México y Colombia. Asimismo, es

Imagen 8: El panorama cibernético nacional.
Fuente: Verint Systems Inc.

importante ubicar esa infraestructura y, por otra parte, será necesario conocer cuáles son las organizaciones críticas, al menos aquellas en las que se puede tener injerencia. En cuanto a las que brindan accesos, deben darse mejores prácticas, suscribirlas e intercambiar información valiosa que puede ayudar en el futuro.

Respecto a las redes nacionales de usuarios, cabe preguntarse si estas son visibles y si es posible controlarlas o monitorearlas. Esta es la parte más difícil del proceso, debido a que entran en conflicto los convenios con las operadoras. Por tanto, tendríamos que responder algunas interrogantes referidas a qué actividades se visibilizan en esta infraestructura maliciosa y quiénes resultarían afectados. A su vez, entra en juego la inteligencia de fuentes abiertas; este es otro punto básico del SOC nacional: contar con personal que monitoree lo que podría suceder, lo que se habla en el momento y responder a las distintas conjeturas suscitadas dentro de un proceso de inteligencia. En ese sentido, no solo es necesario realizar una especie de ciberpatrullaje, sino tener la capacidad de ver dichos elementos y el panorama general, respecto a lo que podría suceder.

A propósito, ¿cuál es el estado del ciberespacio actual? Es necesario saber qué es lo que está sucediendo, quiénes son los actores que intervienen y a los que habría que ponerles la mayor atención. Si tengo identificados a los enemigos, entonces será mi deber monitorearlos. Muchas veces no interesa si se captura a estas personas, ya que lo esencial en este asunto es tenerlos mapeados, para observar al detalle que hacen y no vernos zambullidos en algún problema más adelante.

En cuanto a la organización y operación del centro, aquí les presento una lámina un poco más técnica, sin embargo, les pido que imaginemos una situación en la que debemos monitorear dos sitios con más de dos gigas de tráfico.

Esto genera cinco organizaciones a ser protegidas, millones de eventos al día y millones de Petabytes de almacenamiento. Entonces, ¿cómo analizo todo eso humanamente? Básicamente, y esto ocurre también en el mundo empresarial, la estrategia que han tomado los oficiales de seguridad más exitosos es no detener los ataques durante los dos primeros años de gestión. Suena extraño, pero en dicho periodo se debe conocer, en primer lugar, lo que acontece. Por ello, la inversión debe destinarse a la implementación de acciones de visibilidad —— referido al monitoreo de eventos—— y, en base a ello, se elaborará un plan de contención y respuesta.

Cabe precisar que esto no significa quedarnos de brazos cruzados ante cualquier amenaza, sino que es necesario contar con elementos sustanciales que permitan el monitoreo de ocurrencias dentro del campo visual del centro de ciberseguridad nacional. En una empresa, este proceso resulta muy fácil de implementar debido a su delimitación, a pesar de contar con usuarios remotos, pero, a nivel nacional, es un proceso muy complejo. Empecemos con un sencillo cuestionamiento: ¿tenemos definidas la ciberfronteras? Si así fuese, ¿quién es el encargado de monitorearlas y cerrarlas, ante cualquier emergencia? La frontera de un aeropuerto puede bloquearse ante una emergencia, pero, en el caso del ciberespacio, solo se cuenta con un par de experiencias probadas en las que se decidió cerrar la frontera digital, evidenciándose dificultades en cuanto a la paralización de los servicios internos.

Una solución alterna a esta necesidad sería empezar por reconstruir la historia del ataque, lo cual equivale a preguntarnos qué pasó. La respuesta, obviamente, será “me atacaron”, pero este es un ataque heredado que lleva tiempo gestándose y, por tanto, deberá ser evaluado en torno a sus causas. Un segundo paso será definir el ruido, ya que en el rubro de la ciberseguridad hay demasiadas alertas y componentes, por lo que es necesaria la reducción

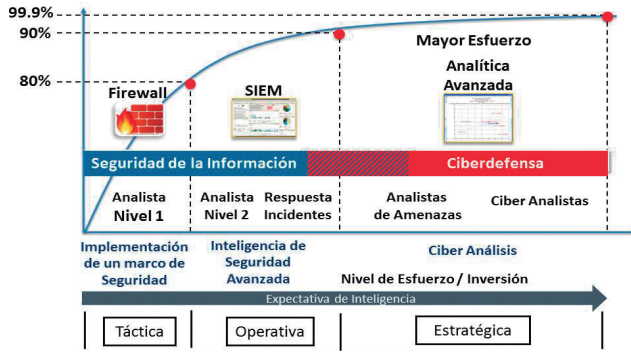


Imagen 9: Inteligencia+Ciberdefensa.
Fuente: Verint Systems Inc.

del ruido que provocan, para enfocarse en aspectos de suma relevancia. Asimismo, es importante contar con rasgos de adaptabilidad en tecnologías de detección y respuesta.

Hace un momento comentaban que el *machine learning* puede ayudar incluso a realizar investigaciones automáticas. Pues bien, otro punto importante en este tema es la inteligencia. Quizás sea posible obtener todo cuanto queramos mediante ese indicador de compromiso, pero la pregunta principal radica en qué hacer con ellos ¿Servirán para publicarlos en una página? Es más, ¿tengo una conexión real con los centros de infraestructura crítica,

Imagen 10: actividades del Centro de Ciberseguridad.
Fuente: Verint Systems Inc.

donde podremos bloquear lo más cercano en tiempo real? Las respuestas enmarcan diversas ventajas, como la observación del panorama completo, el conocimiento de lo que viene sucediendo, la identificación del origen de un ataque (en cuanto a si vino del exterior o se trata de grupo interno) y cuál es el objetivo que puede tener. Aquí entra en juego el conocimiento que ustedes poseen, el cual va más allá de los saberes de las organizaciones empresariales y privadas. Me refiero a la combinación del proceso de inteligencia con las operaciones cibernéticas.

La seguridad es una función asintónica, donde subir es fácil, pero en la que nunca se llega al 100%. Crecer en seguridad es barato al principio, sin embargo, para acercarse a la totalidad del proceso debe ejecutarse un esfuerzo muy complejo y costoso no solo en lo referido al personal y la tecnología, sino en la disposición de todos los que están integrados en el proceso. Ahora, pasamos de la seguridad de la información a la ciberseguridad y ciberdefensa —— recuerden que la cibernética viene de la Marina, del acto de timonear y llegar a buen puerto —— campos en los que se necesitan diversas fuentes de inteligencia; algunas de ellas se vinculan con la inteligencia táctica, referido a lo qué está sucediendo y aquello que puede bloquearse en el momento; la inteligencia operativa, que es una campaña que posee técnicas, tácticas y procedimientos; y la inteligencia estratégica, que podría ser ejemplificada en una situación del mundo empresarial. Supongamos que se abrirá un nuevo ISP, por tanto, será nuestro deber detenernos y observar quien está en contra de dicho sistema.

En cuanto a las actividades del centro de ciberseguridad, es de suma importancia tener en cuenta la política nacional, debido a que esto nos ayudará a determinar sobre qué aspectos se posee injerencia relevante. En base a ello, se desprenden otras evaluaciones, cómo a que agentes se puede monitorear, a quienes se les puede ofrecer el servicio

Imagen 11: el Centro de Ciberseguridad.
Fuente: Verint Systems Inc.

de información y suscripción, así como las investigaciones de riesgos actuales y estratégicos. Consideremos que ejecutar procedimientos de seguridad sin un análisis de riesgo sería como acudir al médico y que nos receten un antibiótico sin tener en cuenta el diagnóstico previo, lo que supondría una peligrosa negligencia. Necesitamos saber cuál es el problema para atacarlo de manera correcta, rastrear continuamente la infraestructura maliciosa y a los autores nacionales, así como generar y distribuir inteligencia de amenazas específicas para los aeropuertos, la Fuerza Aérea, para la Armada y otras organizaciones monitoreadas. De este modo, tomaremos medidas activas de seguridad nacional, en las que pasaremos de la prevención a la ejecución de acciones concretas.

Aquí apreciamos el Centro de Ciberseguridad Nacional. En este esquema, tenemos el área de gestión del SOC nacional, que hace la gestión del centro de ciberseguridad; contamos con analistas junior que observan al detalle las pantallas para reportarnos lo que viene sucediendo; también tenemos a los analistas senior, que son expertos que conocen su labor al detalle y la visualización del campo más allá de lo evidente, en base a una investigación estructurada; en tanto, los analistas forenses conforman

Imagen 12: evolución de las amenazas.
Fuente: Verint Systems Inc.

un equipo que investiga todo lo acontecido y, finalmente, está el equipo de respuesta de incidentes, el cual acude al lugar de los hechos, sea o no de mi organización, para determinar las causas que motivaron lo sucedido.

Estos son recursos escasos y muy costosos, sin embargo, puedo garantizarles que, hoy en día estos elementos son muy cotizados y se los roban de una organización a otra. Bien comentaban hace un momento el problema que supone retener al personal con mayor talento; esto ocurre a menudo en todo el mundo y, por ello, deben evaluarse las condiciones y trazar retos, que no es más que promover la búsqueda de potenciales puntos vulnerables.

La evolución de las amenazas configura un proceso dinámico. Pasamos por la era de los virus hacia los ataques destructivos (como el caso STUXNET), luego vino el tiempo de las amenazas avanzadas, la persistencia de las mismas, el ocultamiento y la era del malware. A propósito, esta amenaza ha crecido en un 360% en el último año, mientras que en las noticias y los conflictos semanales apreciamos discusiones en torno a si IBM o Google poseen la computadora cuántica más rápida, respecto a la ruptura de la criptografía. Por otro parte, se argumentó que una operación que antes tardaba diez

mil horas máquina, ahora se ejecuta en 200 segundos. Esto fue publicado por la NASA y tuvo que retirarlo al poco tiempo de haberlo hecho, debido a la ola de críticas que generó dicho estudio.

El Centro de Ciberseguridad Nacional debe estar preparado para el futuro, sabiendo que estos procesos son tendencia en las organizaciones de transformación tecnológica. Asimismo, debemos implementar un sistema de alertas tempranas, así como iniciar procesos de medición del riesgo nacional y la ejecución del *threat hunting* (o caza de amenazas). En tal sentido, lo que un analista de inteligencia haría en un análisis contextual, al mismo estilo que un analista cibernético, será determinar sus posibilidades y las herramientas con las que cuenta. De este modo, juntará toda esa información y evaluará si existe algo a tomar en cuenta, contando para ello con la inteligencia artificial necesaria; me atrevo a decir que valdría la pena que los expertos se involucren en estos procesos, ya que son muy fáciles de aprender.

Imagen 13: acciones preventivas.
Fuente: Verint Systems Inc.

En cuanto a las acciones preventivas, es interesante observar como el centro nacional genera inteligencia de amenazas para todos los suscriptores y un bloqueo

basado en acciones de inteligencia. Alguno se preguntará cómo se ejecuta esta última acción, pues precisamente a través de la inteligencia; quizás haya dudas respecto a si existen indicadores que uno mismo pueda programar. La respuesta es que hay herramientas en la actualidad que permiten desarrollar esta tarea, sin embargo, es un reto constante.

En cuanto a los retos en ciberseguridad, más de uno se pregunta cómo logar la visibilidad de la llamada *backbone* nacional. Cabe mencionar que el Centro de Ciberseguridad Nacional es un proyecto ambicioso en el cual es posible determinar el acceso a la visualización del tráfico de una nación y su pertinente monitoreo de las acciones acaecidas. Por ello, es necesario encontrar una forma de integración con la infraestructura de terceros para, al menos, tener la visibilidad de dicho campo y bloquearlo si es necesario. Bien sabemos que se necesita de mucha colaboración en esta actividad, ya que en ocasiones no solo se requiere del intercambio de oficios, sino ejecutar acciones bajo decisiones informadas; esto es muy complicado, pero representa el futuro.

Alguno de ustedes recordará cuando la conexión a internet se realizaba mediante el módem y la calidad de las imágenes en 1995, las cuales eran ASCII y tardaban muchísimo en descargarse. Uno veía la imagen con cierto desgano mientras bajaban de 14k a 9k de velocidad, sin embargo, hoy en día se puede robar toda la base de datos de un banco a través de un ADSL en un par de horas, por lo que la reacción de debe ser mucho más rápida. El problema sigue siendo el mismo, pero es obligatorio responder casi de forma instantánea.

sesión

1.2

Aplicación práctica e implicaciones de las operaciones del ciberespacio de guerra

C. de N. USN (r)
Alfred Turner

El Almirante White y la Doctora Nina Kollars, nos han presentado el ciberespacio desde un punto de vista amplio, mientras que el señor Pérez del Real llevó el tema al ámbito nacional, por ello, continuaré en el mismo camino, pero en dirección descendente. Mi tarea es enlazar el ciberespacio con el dominio marítimo, que es específicamente de donde provengo. He trabajado en la US Navy por treinta años y la mayor parte de mi carrera la desarrollé en operaciones tradicionales como la guerra aérea, de superficie y submarina; por otro lado, fui comandante del componente de ciberdefensa de mi Marina y precisamente, durante mis últimos diez años de carrera, el objetivo de mi trabajo fue juntar el campo tradicional con el ciberespacio.

Ciberespacio: "La red interdependiente de infraestructuras de tecnología de la información, que incluye Internet, redes de telecomunicaciones, sistemas informáticos, y procesadores y controladores integrados." (Oficina del Director de Inteligencia Nacional -ODNI, 2018)

Información: crear, almacenar y transmitir

Efectos físico

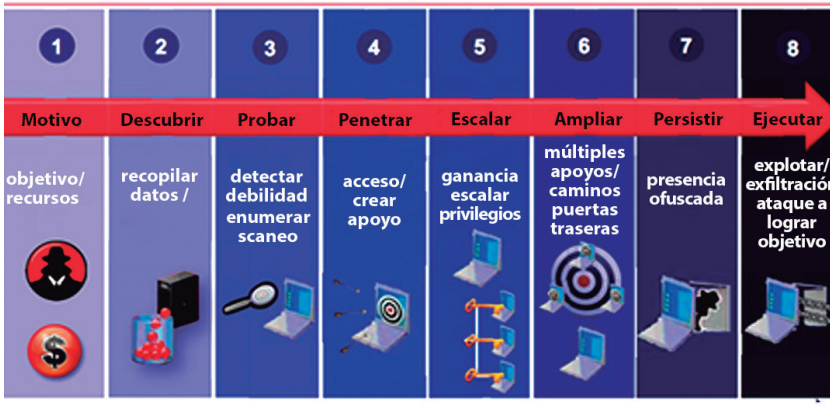
La actividad humana en el ciberespacio es (principalmente) la misma que en el espacio físico

Imagen I : ciberespacio
Fuente: expuesto por el autor.

Antes de continuar con este viaje, les diré que la palabra "ciberespacio" genera diferentes definiciones en la mente de cada persona. En mi caso, prefiero verlo como una red compenetrada con los equipos que hay en ella; la doctrina de los Estados Unidos y la teoría señalan que el ciberespacio incluye la capa lógica y otros estratos, sin embargo, prefiero

simplificar esta concepción en cuanto que el ciberespacio es un dominio de actividad humana, de combate y de guerra. En ese sentido, un agente es capaz de realizar diversas actividades en este dominio, como crear, almacenar y transmitir información o producir algún efecto físico.

Todos estamos conectados con nuestros dispositivos y estos, a su vez, también lo están. Yo puedo prender la alarma de mi casa, encender las bombillas de luz y, en otro ámbito, podría hacer navegar buques, activar o apagar la propulsión y cambiar la velocidad de una nave desde el puente de comando, debido a que todo se encuentra interconectado. Esto evidencia la generación de efectos físicos y de información, pero el punto central es que, al ser un dominio de actividad humana (en el que uno es capaz de ver lo que pasa en el espacio cibernético), todo lo que ocurra en el ciberespacio tendrá un efecto análogo en el espacio físico.



objetivo / efecto deseado
Actividad criminal
Recopilación d información

- Robo de propiedad intelectual
- Funciones de operaciones de soporte

Ataques / empleo de la fuerza

- Guerra electrónica
- Operaciones de información
- Infraestructura en la costa (redes comerciales, ICS /SCADA)

Buques y embarcaciones

- Redes administrativas
- Control o engaño HM&F
- (Sistemas de casco, mecánica e ingeniería)

Imagen 2: Anatomía de ataque.
Fuente: expuesto por el autor.

Imagen 3: marco de amenaza al dominio marítimo.
Fuente: expuesto por el autor.

Empezaré mi exposición mencionándoles cuales son los tipos de amenazas presentes en este campo: existen los que afectan a los militares, a las marinas y también a la industria militar.

Estos son amenazas que se manifiestan en el ciberespacio y que se interceptan con el dominio militar, tal como sucede con las actividades criminales. Menciono esto porque el nivel de efecto es bastante fuerte en estas acciones; por ejemplo, lo primero que debemos determinar el objetivo y a los actores en el ciberespacio, así como lo que pretenden lograr. Por otro lado, necesito saber quiénes son los responsables: ¿se trata de criminales?, ¿son actores no estatales, organizaciones terroristas, extremistas o acaso una actividad fuera de la nación?

Por fortuna, existen dos componentes para identificarlos: en base a lo que están haciendo estos actores y si cabe la posibilidad de que operen desde actividades vinculadas a la inteligencia. Es importante poner énfasis en este último punto, pues el ataque podría darse desde la óptica

de la Marina o detrás de las compañías que construyen las plataformas. Por otro lado, es posible que ellos estén intentando manejar inteligencia en mis actividades de operaciones; en consecuencia, es necesario entender cuáles son mis vulnerabilidades, ya que podrían actuar más rápido que la respuesta que podríamos ofrecer. Culminado esto, el siguiente paso sería el ataque o el uso de la fuerza.

Cabe mencionar que los retos en un ataque o en el proceso de inteligencia dentro del ciberespacio son muy similares a los pasos dados por el actor plenamente identificado. En ese sentido, es necesario entender la figura total en cuanto a las motivaciones del atacante, respecto al ciberespacio. Por otra parte, es necesario entender qué es lo que motiva a este actor en el ciberespacio, lo que podría hacer en otros dominios y cuáles son sus objetivos. Por otro lado, debemos especificar si los agentes operan dentro de la nación o son criminales extremistas; esto nos dará una idea respecto a si las actividades de inteligencia enemigas representan un ataque o un asunto personal.

No olvidemos que, cuando hablamos del ciberespacio, hacemos referencia a la guerra electrónica desde la perspectiva de los Estados Unidos. Este concepto forma parte de la guerra de la información, la cual forja una alianza con las operaciones en el ciberespacio.

Respecto a las operaciones de información, en muchos artículos se les confunde con las operaciones del ciberespacio, pese a que una diferencia sustancial entre las acciones físicas que se ejecutan en el ciberespacio y las de información. En cuanto a las actividades desarrolladas en el ciberespacio, los ataques puedan dañar infraestructuras costeras, el sistema administrativo, redes de gerencia, el sistema de control de las industrias, el sistema que controla las grúas o cualquier mecanismo mediante el cual opera un puerto. Lo peor de todo esto es que existen amenazas directas hacia naves militares o comerciales.

De acuerdo a estos planteamientos, debemos establecer si los ataques configuran una amenaza para el sistema administrativo o para los navegantes que manejan los sistemas y todos los componentes de ingeniería de la nave, junto con sus comandos de control. Sin embargo, el punto central de esta idea es que, nuevamente, debemos definir quiénes son nuestros adversarios.

Imagen 4: recopilación de información:
Fuente: expuesto por el autor.

Ahora bien, la recopilación de información (entendida como una labor de inteligencia) es distinta en el ciberespacio, debido al acceso, la escala y la variedad de los actores que la ejecutan. Sin embargo, estos agentes no necesitan entrar a un determinado país para recabar datos, lo que significa que prescinden del rompimiento de barreras físicas de seguridad para acceder a los registros, archivos y a todo lo que se desea proteger. Una vez conseguido el objetivo, no es necesario que el atacante fotografíe el material sustraído, ya que, o bien saca la información de su lugar de origen, o la descarga aun estando a miles de millas de distancia de la computadora intervenida. Entonces, será de

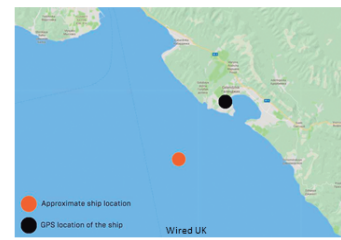
vital importancia establecer las implicancias operacionales directas.

Ellos bien podrían acudir a los contratistas que construyen naves, submarinos, aviones y copiar sus diseños. Obviando los costos de investigación, podrían obtener las mismas capacidades que cualquier país del mundo, incluso del nuestro. Por ejemplo, ¿han pensado que sucedería si una nave de guerra quedase sujeta a un ataque continuo por otro país? Por eso, necesitamos saber si existe otra nación con las mismas capacidades respecto a naves y armamento.

Asimismo, debemos identificar nuestras vulnerabilidades y los sistemas tradicionales de trabajo y luego analizar las implicancias operacionales directas —una de estas sería, por ejemplo, la infiltración del adversario en las redes, permitiéndose tomar decisiones más rápido que nosotros—. Partiendo de este último caso, queda

- Jamming/interferencia de GPS:
  - Estrecho de Ormuz, Ag. 2019 (Irán)
  - Este del Mediterráneo, Nov. 2018 (Rusia)
  - Mar de Barents y Mar de Noruega, Oct. - Nov. 2018 (Rusia)
  - Mar de Azov y Mar Negro, Jun. 2017 – periódico (Rusia)

- Comunicaciones y Radar
  - Despliegues, ejercicios y desarrollo de capacidades en China
  - Integración rusa de capacidades de Guerra Electrónica



Requiere capacidades resilientes y redundantes para operar en un entorno electromagnético desafiante

Imagen 5: guerra electrónica.
Fuente: expuesto por el autor.

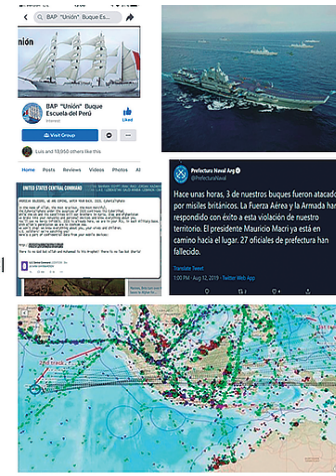
comprobada la necesidad de defender las redes. Asimismo, debemos asegurarnos que las compañías y personas con las que lidiamos a diario sean de entera confianza; por otro lado, tenemos que proteger y defender las plataformas.

Permítanme mencionarles que la guerra electrónica difiere, en ciertos aspectos, con las operaciones tradicionales. Por ejemplo, a comparación de cinco años atrás, el sistema GPS se ha convertido en un sistema integrado a la navegación de hoy en día. Ante esta nueva tecnología, las amenazas no tardaron en llegar. Clara evidencia de ello son las interferencias en la señal de GPS ocurridas en el Estrecho de Hormuz, en el Mar de Barents, en el Mar Negro y en el Mar de Azof. En el caso del tercero, se reportó una emergencia en un buque mercante que atravesaba dicho mar, sin embargo, la posición que arrojó el GPS colocaba a la embarcación sobre tierra y no en el mar.

Esto representa una extensión de la guerra electrónica convencional, en un entorno en el que depositamos nuestra confianza en los sistemas electrónicos de navegación. Por ello, necesitamos ser resilientes para adaptarnos a todos estos problemas y operar en este escenario de señales. Asimismo, debemos ser capaces de operar sin estos dispositivos electrónicos y, para ello, el personal tiene que ser diestro en cuanto a la navegación en un ambiente adverso.

Las operaciones de información marítima pueden ser amigables o potencialmente hostiles nuevamente. Esto es algo establecido desde hace cientos de años, pero es necesario que establezcamos algunas diferencias entre ellas. Precisamente, difieren en base al adversario que se tiene en frente, ya que el ciberespacio brinda la capacidad y habilidad para amplificar diversos mensajes; tuve la oportunidad de ver en Facebook estas fotografías que muestran el BAP Unión y así como puedo ver que es lo que se está haciendo (debido a que la información pasa al dominio público en una red social) hay medios

- Diplomacia naval y seguridad marítima
  - Influir en amigos y adversarios; impedir la actividad ilícita
  - El ciberespacio proporciona la capacidad para amplificar el "mensaje"
- Riesgo de las redes sociales
  - Hackeo de la cuenta de Twitter de la Armada Argentina, Ag 19
  - Hackeo de las cuentas de Twitter y YouTube del Mando Central de los Estados Unidos (USCENTCOM), En. 15
  - Cuentas personales del personal del servicio
- Engañar o evitar ser detectado
  - Medidas tradicionales de control de emisiones de señales, radares y / o comunicaciones
  - Falsa identificación de AIS



Una simple operación de información puede tener efectos significativos

Imagen 6: operaciones de información marítima.
Fuente: expuesto por el autor.

sociales en el ciberespacio que echan mano de esto para el beneficio de otros países. De acuerdo con ello, soy enfático en afirmar que el ciberespacio ofrece múltiples oportunidades de acción, pero trae consigo un sinnúmero de vulnerabilidades.

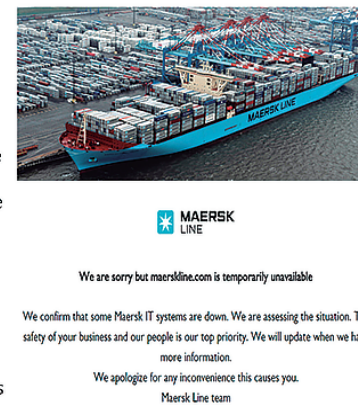
Este fue el caso de la Armada Argentina, la cual fue hackeada durante el lapso de diez minutos. Cientos de personas vieron información falsa en la cuenta de Twitter de la institución, la cual pudo tener implicancias nacionales muy severas para la Marina de Argentina. Un caso similar ocurrió en el centro de comando en Estados Unidos, cuando las cuentas en las redes sociales empezaron a vertir mensajes falsos.

En otro ámbito, tenemos la detección tradicional de los comandos y controles o las misiones de control, en las que se puede operar desde el silencio, existiendo en la actualidad muchas maneras de llevar a cabo dicha tarea, como la colación de banderas falsas. Todo esto trasciende

desde las naciones a los actores independientes, ya sean criminales u otro tipo de organización. Por ejemplo, tenemos números de identificación con el sistema AIS, en los que se visualiza el nombre de la nave o del buque, pero estos tienen una bandera falsa o presentan pseudónimos en sus denominaciones. No debemos olvidar que hay personas detrás que tratan de conducir actividades criminales, como en el caso de los buques que ejercen la pesca ilícita en aguas prohibidas.

Ahora pasemos a las grandes amenazas. Probablemente estén familiarizados con lo que paso en la empresa Maersk en junio del 2017; fue un ataque no deliberado, el cual dañó la infraestructura del puerto de una compañía naviera mundial. Este hecho llamó a la reflexión a muchos, pues es probable que un hecho similar ocurra en la estructura de una

- Ataque versus red comercial marítima/ infraestructura en tierra
  - Malware destructivo NotPetya; Rusia
  - Acciones inmediatas de MLL; desconectar
  - Impacto en las operaciones; comerciales y portuarias
- Observaciones y detalles
  - Resiliencia limitada en operaciones manuales y de red
  - Seguimiento de la carga es un desafío importante
  - Efectos temporales pero costosos; semanas/meses para que MLL se recupere; relaciones personales críticas
  - Riesgo de la industria equivale al riesgo militar
- Camino por recorrer
  - Reconstruir y mejorar la red
  - Acuerdos de intercambio de información entre los operadores estadounidenses y el Ministerio de Defensa de los EE. UU.; futuro apoyo del Ministerio de Defensa
  - Acuerdos contractuales que especifican los requisitos de ciberseguridad y defensa



Seccionar redes; estar preparado para operar la infraestructura crítica en tierra de forma manual

Imagen 7: MAERSK line ltd. (MLL), 27 de junio del 2017.
Fuente: MAERSK line.

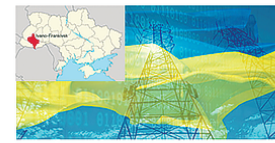
marina de guerra. El sistema de administración no clasificado de Maersk quedó comprometido y, posteriormente, destruido, lo cual generó un daño colateral muy grande. Las investigaciones revelaron que el ataque configuró una operación de información, siendo esta la magnitud de lo que puede hacer un adversario a través de las redes, desde una perspectiva física e informática. Esto ocasionó un daño severo tanto en la infraestructura de Ucrania como en Maersk, ya que fueron destruidas todas sus redes de negocios, lo que ocasionó que los funcionarios operasen con papel y lápiz; se perdió el acceso a todos los archivos y se vieron obligados a reconstruir la red en semanas. Esto fue posible gracias a que uno de los controladores principales del dominio tenía la imagen de la red y, durante el ataque, se encontraba fuera de línea por un problema eléctrico. Sin este golpe de suerte, hubiese sido imposible rehabilitar el sistema. Cabe mencionar que Maersk, en el año 2014, ya consideraba el aspecto ciber como un potencial riesgo y afirmaron que venían preparándose para afrontarlo. Tres años después, perdieron toda su red.

Respecto a las mejoras que podríamos implementar al proceso, están las acciones de protección de redes, así como su segmentación, hecho que cualquier operador debe tomar en cuenta. Por otro lado está el desarrollo de actividades básicas, para ganar confianza en dicho campo, siendo el primer paso de estas la capacitación y entrenamiento del personal en manejo de redes.

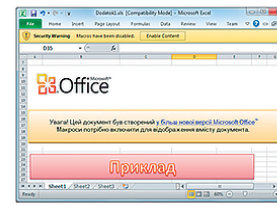
En la actualidad, Maersk viene reconstruyendo su sistema y cumpliendo lo prometido en el 2014, ya que el ataque produjo un aproximado de 300 millones de dólares en pérdidas. Esto no solo afectó a Maersk, sino también a muchas otras compañías; el costo dirigido al comercio mundial le costó a la empresa billones de dólares después del ataque. Visto este caso, no es necesario discutir sobre la amenaza que suponen estas acciones para nuestras redes de trabajo en las marinas, o para las infraestructuras de apoyo.

Otro suceso relevante tuvo lugar en Ucrania, durante los años 2015 y 2016, cuando el país estaba en conflicto con el sector de Ucrania oriental. Los agresores atacaron todo el sistema de infraestructura, teniendo como objetivo escalar en este conflicto. Este es un claro ejemplo de como el ciberespacio es utilizado para alcanzar objetivos de guerra

- Antecedentes
  - Conflicto en Ucrania oriental; cortes de energía en Crimea
  - Malware Black Energy versus elemento ICS/SCADA de la infraestructura de energía eléctrica de Ucrania
  - Objetivo ruso: socavar el apoyo popular al gobierno de Ucrania y apoyar a la población prorrusa
  - Cambio a controles manuales



- Detalles
  - 230K personas sin electricidad 1-6 h
  - Respaldo manual crítico; aún necesita un plan de respaldo
  - Ataque limitado en amplia coordinación con otros medios de "conflicto de zona gris"
  - Efecto estratégico y operativo limitado de forma aislada pero eficaz como parte de la campaña general



Los sistemas HM&E en plataformas son vulnerables a ataques a través del ciberespacio; minimizar y asegurar las conexiones; ser capaz de operar de forma manual

Imagen 8: Ucrania.
Fuente: expuesto por el autor.

hibrida. El sistema de generación eléctrica ucraniano quedó totalmente paralizado y es muy probable que los actores de Rusia hayan pasado seis meses preparando el primer ataque y otros seis elaborando la segunda parte de la operación. Y es que no solo tomaron el control de las computadoras para apagar todas las estaciones de energía, sino que destruyeron el sistema de suministro eléctrico, tomando el control de las redes de energía y dejando a la ciudad sumida en la penumbra. Sin embargo, cabe mencionar que el efecto del ataque solo duró seis horas, debido a que los ucranianos tenían un sistema de energía antiguo disponible.

Ahora que hablamos de eso, he visto cierta similitud con los buques antiguos. Si el barco tenía componentes modernos, era posible acceder a sus controles y conectarlos de forma manual. Precisamente esto hicieron los ucranianos al desconectar todos sus cables y conectarlos manualmente al sistema eléctrico. Imagen todo ese efecto en cascada y preguntémonos las consecuencias físicas que hubiese ocasionado la avería, si es que los ucranianos esperaba que el sistema eléctrico regresase en, aproximadamente, seis meses.

Les comento esto porque confiamos a ciegas en nuestros sistemas, en la infraestructura y generación eléctrica desde cierto punto de vista. Por ello, se necesita mucha imaginación para comprender que poseemos sistemas similares en nuestros barcos, los cuales cuentan con

Infraestructura marítima en tierra

- Ciberataque de EE.UU contra Irán, jun. 2019
- Ciberataque simulado por el Comando Central contra un puerto marítimo, jun. 2019.
- IRasonware Puerto de San Diego, sep. 2018

Ciberataques versus sistemas de control de los buques y las redes administrativas

- Se intenta tomar el control de M/V en ruta Nueva York / Nueva Jersey, feb. 2019.
- Alertas de la Guardia Costera de los EE.UU, 2019
- Avisos del sector marítimo civil desde 2014
- Secuestro del sistema de navegación de yates, verano 2013

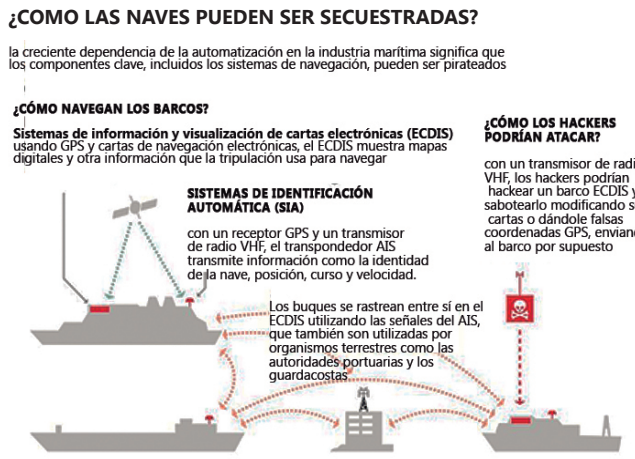


Imagen 9: amenaza a la infraestrutura crítica y a las naves.
Fuentes: Reuters, Organización Marítima Inernacional de Tráfico Marítimo.

estaciones eléctricas, como el caso de Ucrania, y que están conectadas en algún lugar del ciberespacio. Es posible, entonces, que exista un actor que eventualmente podría causar daños a nuestros sistemas de navegación, ingeniería o al sistema de armas. A simple vista, parecen situaciones extraídas de la ciencia ficción, pero, hoy en día, estas amenazas abarcan el entorno de la realidad.

Una situación concreta de esto fue un caso en el que, según las noticias, Estados Unidos condujo un ciberataque contra Irán, probablemente en respuesta a una actividad ejecutada en el estrecho de Ormuz. En dicho ataque se habría destruido la base de datos de una entidad dedicada el traqueo de buques mercantes, por lo que tuvieron la capacidad de manejar estas operaciones. En el último año, hemos visto ejercicios de ciberataques en los puertos marítimos, lo que demuestra como nuestros puertos son vulnerables.

En otro punto, tenemos también la amenaza del ransomware, tal como mencionaron los expositores que me antecedieron. En los puertos de San Diego y Barcelona, por ejemplo, tuvieron lugar ataques criminales que impidieron las operaciones de estos terminales por más de un día. Cabría preguntarnos, entonces, qué pasaría si perdiésemos la habilidad de visualizar y acceder a los registros de comercio o al sistema logístico, ¿seríamos capaces de seguir operando en ese ambiente? Por otra parte, una empresa china pasó por la misma situación que Maersk, con la diferencia de que fueron capaces de mantener sus operaciones de manera exitosa.

En el caso de ataques a los barcos, en una ocasión los Guardacostas de Estados Unidos informaron que un buque sufrió un incidente, debido a que trataron de trataron de tomar el control de la embarcación desde el ciberespacio, a través de las redes.

En cierta ocasión, los profesores de la Universidad de Texas desarrollaron un experimento en base a capacidades muy básicas y equipos disponibles. De este modo, fueron capaces de inyectar información diferente al GPS de un barco, sin tocar ninguno de sus componentes, dirigiéndolo hacia dónde ellos querían. Si alguno de los actores viese que esto pasó hace solo cinco años, tengan por seguro que continuarán trabajando sobre lo ya hecho, con el fin de desarrollar nuevas capacidades.

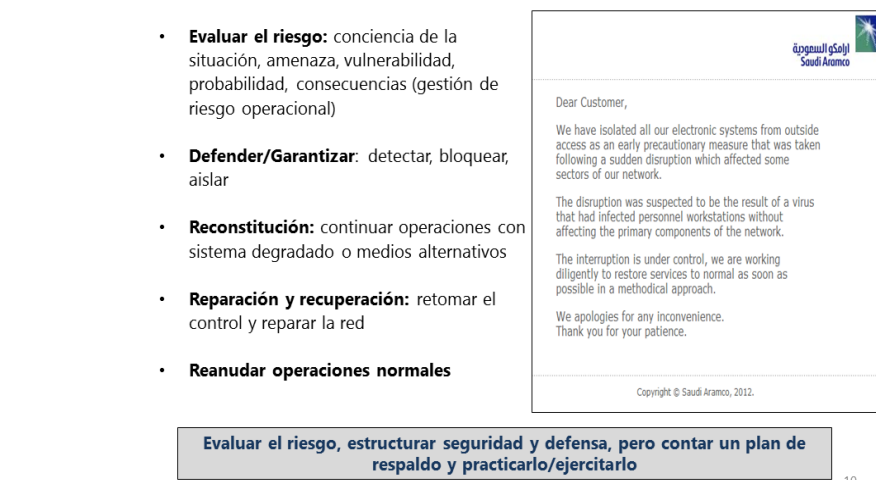
Puede que el panorama les parezca sombrío, pero créanme cuando les digo que no todo está perdido. Si deseamos conseguir un adecuado marco de seguridad en el ciberespacio, debemos tener en cuenta que las amenazas no son iguales. Asimismo, debemos analizar el riesgo, tomando pleno conocimiento de la situación: tenemos que conocer la red, así como entender las amenazas y vulnerabilidades. Del mismo modo, debemos entender cuáles serían las consecuencias y probabilidades de que un evento suceda, así como el tratamiento de la contingencia y el arreglo de la red en el ciberespacio, priorizando siempre las operaciones pertinentes.

Por otro lado, tenemos que defender y asegurar nuestro ciberespacio, con el fin de detectar la amenaza, bloquearla y aislarla. En tanto, la segmentación y aislamiento de redes es otro punto necesario para el aseguramiento; necesitamos establecer contraseñas efectivas e interiorizar conceptos de seguridad que nos permitan capacitar al personal encargado de las operaciones de las redes acerca de la realidad en torno a los ataques.

Asimismo, es muy probable que, en algún momento, las defensas de nuestras redes fallen. Por eso, resulta de vital importancia saber cómo proceder de forma manual, si es que llegásemos a enfrentar una situación de tal magnitud; de esa manera, será posible manejar los puertos independientemente del sistema de información afectado, ayudaremos a los buques a navegar sin GPS,

controlaremos las plantas de ingeniería sin una pantalla táctil o una computadora, manejaremos el sistema de armas sin información y todo esto debido a que los sistemas podrían estar comprometidos de algún modo por el ataque. Por ejemplo, un ataque podría afectar al sistema administrativo y esto generaría una gran preocupación, puesto que el sistema de operaciones sufrirá variaciones que no permitirán el acceso a información valiosa. Es en ese momento que necesitaremos dilucidar como arreglar el desperfecto para que la red entre en servicio y recuperar el control sobre el dominio. Para ello, será necesaria la presencia de personal eficiente, debido a que el ciberespacio es muy grande y se necesita construir sistemas más eficientes para adecuar las condiciones de trabajo. De este modo, seremos capaces de evaluar los riesgos de la defensa, siempre y cuando tengamos un respaldo sólido para casos de emergencia.

Por otro lado, debemos ser proactivos en la respuesta hacia las amenazas. Pongan atención en ello, pues no solo



- **Evaluar el riesgo:** conciencia de la situación, amenaza, vulnerabilidad, probabilidad, consecuencias (gestión de riesgo operacional)
- **Defender/Garantizar**: detectar, bloquear, aislar
- **Reconstitución:** continuar operaciones con sistema degradado o medios alternativos
- **Reparación y recuperación:** retomar el control y reparar la red
- **Reanudar operaciones normales**

Evaluar el riesgo, estructurar seguridad y defensa, pero contar un plan de respaldo y practicarlo/ejercitarlo

Imagen 10: marco de seguridad del ciberespacio.
Fuente: expuesta por el autor.

en el ciberespacio ocurren contingencias: pueden darse en el ámbito militar, en el campo civil o del Gobierno. En todo caso, tenemos que ser capaces de contrarrestar las amenazas y anticiparnos a ellas.

Lo ideal en este proceso sería que los gobiernos compartan informaciones con sus socios responsables, en torno a las amenazas que han enfrentado o de aquellas que los acechan dentro del Gobierno, en el sector militar y privado. Esto es lo que hacemos en Estados Unidos, cuando se cuenta con información disponible.

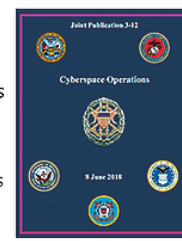
Luego, necesitaremos saber quién es el encargado de la defensa del ciberespacio en un determinado país, debido a que lidiaremos constantemente con sus tareas. En este dominio es difícil saber cuáles son las fronteras y es materia de discusión también cuáles son las líneas rojas que constituyen una actividad en la que se necesita ser reactivo o no. Tengamos en cuenta que este es un espacio

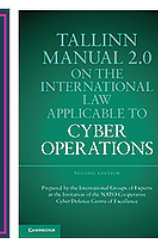
¿Qué se puede hacer dentro de nuestras fuerzas?

- Invertir desde el principio en ciberseguridad y defensa para infraestructura y plataformas
- Educar, capacitar y realizar ejercicios personal/organizaciones
- Compartir datos de amenazas y mejores prácticas
- Mostrar proactividad ante la respuesta a amenazas

¿Qué nos gustaría que hicieran nuestros gobiernos?

- Compartir datos sobre amenazas y mejores prácticas en sectores gubernamentales, militares y civiles, e internacionalmente con socios
- Garantizar la transparencia en las funciones y responsabilidades nacionales
- Continuar definiendo los marcos internacionales aplicados al ciberespacio.





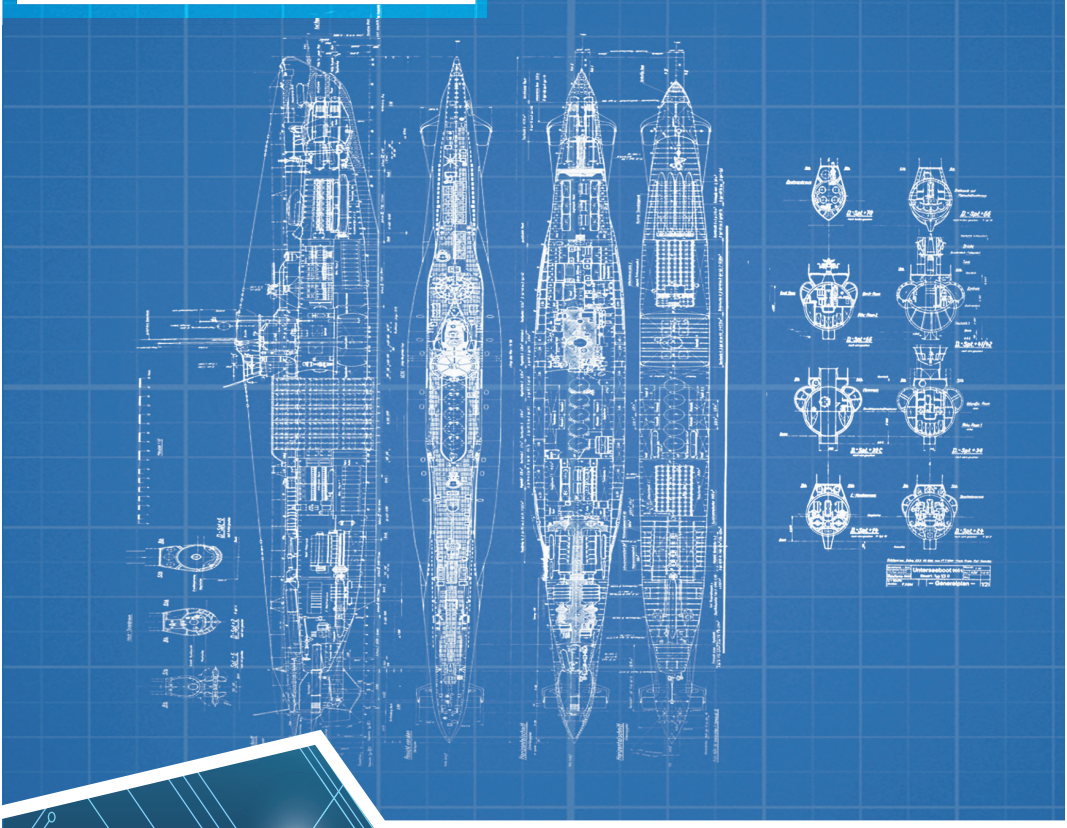
Utilizar los mecanismos existentes para ayudar a determinar el camino a seguir; las analogías son como estrellas con las que se puede navegar

Imagen II: operaciones y seguridad en el ciberespacio.
Fuente: expuesto por el autor.

nuevo y no funciona como hace diez o quince años atrás. En ese sentido, a nivel internacional no existen estándares ni un acuerdo común de leyes que rijan el uso del ciberespacio. El establecimiento de las mismas ayudaría mucho en cuanto a la confianza de operaciones en este ámbito.

Concluimos entonces que la lección aprendida es que las actividades desarrolladas en el ciberespacio configuran una acción humana y, por tanto, producen un impacto físico. Hay gente que discute a menudo cuáles son las reglas, políticas, estrategias y las bases que nos guíen al correcto desarrollo de las actividades en el ciberespacio, siendo conscientes de sus efectos posteriores. Es necesario que todos estemos familiarizados con estos conceptos, pues sirven de ayuda para entender lo que está pasando a nuestro alrededor y, en base a ello, seremos capaces de navegar hacia buen puerto, a través de la inmensidad que ofrece el ciberespacio.

CONSTRUCCIONES NAVALES



ESCUELA SUPERIOR DE GUERRA NAVAL

V SIMPOSIO INTERNACIONAL DE SEGURIDAD Y DEFENSA

PLANO 1

Fecha: 25-09-19

Humberto Caldas da Silveira Junior

Roger Berg

Juan Carlos Diaz Cuadra

Paolo Tornese

BLOQUE 2

BLOQUE 2

MODERADORES

EXPOSITORES

SESIÓN 2.1

Calm.
Percy
Pérez Bramosio

La Marina de Guerra del Perú opera con submarinos desde el año 1911, habiéndose celebrado en el mes de agosto los 108 años de existencia de la División de Submarinos, la cual se convirtió posteriormente en la Flotilla de Submarinos y luego en la Fuerza de Submarinos.

Durante este periodo, se ha producido un continuo aprendizaje y la incorporación de tecnología necesaria para el mantenimiento de nuestras unidades submarinas. A continuación presentaré un breve recuento.

La vida operativa de los sumergibles franceses Lebauf (que fueron nuestros primeros submarinos) se vio limitada debido a que las labores de mantenimiento tuvieron que realizarse en astilleros extranjeros sumado a que, cuando las unidades requirieron trabajos de recorrido y el primer cambio de baterías, dicho proceso coincidió con el estallido de la Primera Guerra Mundial.

Posteriormente, entre 1926 y 1928, se adquirieron en los Estados Unidos de América los submarinos “R”, los cuales hicieron sus recorridos y cambios de baterías en Norteamérica de forma periódica, específicamente en el astillero constructor de la Electric Boat Corporation. Asimismo, de abril a diciembre de 1950, los cuatro “R” retornaron a New London a realizar trabajos de recorrido integral y fueron sometidos a labores de modernización de equipos y sistemas principales; en este proceso, se instalaron nuevos sonares, radares y el eyector de señales. Estas unidades operaron hasta 1958, fecha en que se les dio de baja.

Las unidades tipo “R” fueron reemplazadas por las de tipo “S”, las cuales realizaron sus primeros reemplazos de baterías y recorridos en los Estados Unidos de América, hasta que en 1966 el Servicio Industrial de la Marina (SIMA) llevó a cabo la variación de las cubiertas de popa fija a rebatibles e inició los recorridos y cambios de baterías en el Perú. El primer corte en el casco resistente de un submarino se ejecutó en el año 1969 sobre el B.A.P. Angamos SS-43, con la finalidad de generar la transformación de los embragues neumáticos.

En 1974, cuando la Marina de Guerra del Perú adquirió dos submarinos clase Guppy, el B.A.P. La pedrera fue reactivado e inició recorridos en los Estados Unidos de América, mientras que el B.A.P. Pacocha fue remolcado por el buque Guardián Ríos desde Filadelfia al Callao, realizándose su reactivación en el SIMA del primer puerto.

En 1974 y 1975, los buques Arica e Islay, que fueron nuestras primeras unidades tipo 209, quedaron comisionadas. A comienzos de los ochenta, cuando estos submarinos necesitaron su primer reemplazo de baterías y empezar con sus recorridos, dichos procesos se efectuaron en el astillero constructor HDW en Kiel, sin embargo, años más tarde, a inicios de los noventa, cuando las unidades clase Angamos requirieron el primer cambio de baterías y los de clase Islay el segundo, se tomó la decisión de realizar los trabajos en el SIMA.

Por ello, el B.A.P. Pisagua efectuó su primer recorrido y sustitución de baterías de una unidad submarina tipo 209 en el Perú, en el año 1992, proceso que se aplica hasta el día de hoy y que viene ampliándose paulinamente en cuanto a la complejidad y profundidad de los trabajos.

Más adelante, en el año 1996, se desarrolló el primer injerto en un casco resistente de acero HY-80, así como la recuperación con soldadura de los monoblocks de aluminio de los diésel MTU 12V493AZ-80.

Del mismo modo, en el año 2013, gracias a los proyectos de investigación y desarrollo iniciados para combatir la obsolescencia de los sistemas a bordo se instaló en las unidades clase Islay el sistema SSSCT, el cual reemplazó a los VM-8 y, en el año 2015, se instaló el primer sistema de combate Kallpa en el B.A.P. Angamos, el cual reemplazó a la SIMBADS. Esto supuso el comienzo de los desarrollos de diversos sistemas con tecnología propia.

Este largo proceso de aprendizaje permitió que en el año 2017 iniciara la modernización de las unidades clase Angamos a cargo del SIMA – Callao, con el apoyo técnico de TKMS y empleando un alto grado de componentes nacionales.

En la región, Brasil es el país que ha logrado los mayores avances en el campo de los submarinos, ya que consiguió desarrollar una adecuada infraestructura y gracias a ello obtuvo la experiencia necesaria para la construcción de unidades submarinas. Por otro lado, sabemos que en el arsenal de Rio de Janeiro se ejecutó la construcción de unidades tipo 209 – 1400, como el caso del Tamoio en 1994, Timbira en 1996, Tapajó en 1999 y el Tikuna en el 2005.

Asimismo, como parte del Programa de Desarrollo de Submarinos (PROSUB) se construyó el Complejo Industrial de Itagüí, para la producción de submarinos convencionales de la clase Scorpene y una unidad nuclear,

habiéndose lanzado en diciembre del 2018 la primera unidad de este tipo llamada Riachuelo.

El día de hoy contamos con interesantes exposiciones respecto al tema de los submarinos, como la que sostendrá el Almirante de la Marina de Brasil Humberto Caldas Da Silveira Junior, quien nos hablará de la experiencia submarinista de su país. A continuación, tendremos con nosotros al doctor Roger Berg, del astillero sueco SAAB, centro que cuenta con más de cien años de experiencia en el diseño y construcción de unidades submarinas, entre los que podemos mencionar los submarinos de la clase Vastergotland y Gotland Suecos, el clase Collins, construido para Australia, y el nuevo A-26. El doctor Berg disertará sobre el sigilo en las unidades submarinas y la tecnología empleada para la reducción de la firma acústica y magnética en el diseño y construcción de submarinos.

sesión

2.1

El Complejo Naval de Itaguaí: la infraestructura y la construcción de submarinos

Calm.
Humberto Caldas
Da Silveira Junior

En nombre de la Marina de Brasil, agradezco a la Marina de Guerra del Perú por la oportunidad brindada para presentar nuestro proyecto. En tal sentido, disertaré acerca de lo que hicimos y lo que venimos haciendo en la actualidad al interior de la institución. Como mencionó el Almirante Pérez, esta iniciativa es ambiciosa y llevamos diez años trabajando duro para concretarla.

A continuación, expondré algunos puntos respecto a las nuevas fronteras de la defensa brasilera, el Programa de Submarinos (Prosub) la infraestructura industrial, la construcción de los submarinos y, adicionalmente, comentaré sobre la situación del submarino de propulsión nuclear, el cual pretendemos construir en el transcurso de la próxima década.

El entorno estratégico de interés principal en Brasil, así como para nuestra Marina, es la Amazonia Azul. Dicho concepto fue enunciado hace quince años con la finalidad de brindar una visión integral a la sociedad civil, a los dirigentes civiles y políticos sobre la importancia de nuestro mar territorial, la zona económica exclusiva y la plataforma continental en frente de Brasil y dentro del Atlántico Sur.

Cabe mencionar que esta es un área muy grande y representa el 10 % del tráfico marítimo mundial, lo que equivale a un 67 % del territorio terrestre brasileño; casi el 97 % de nuestras importaciones y exportaciones a países de América del Sur, a los Estados Unidos de América, Europa y Asia pasan por nuestra Amazonia Azul. Precisamente, el 95 % de nuestro petróleo es extraído del mar y en los últimos diez años extrajimos el recurso de la camada Pre-Sal, ubicada a cinco mil metros de profundidad. De este modo, extraemos diariamente algunos millones de barriles y las perspectivas en torno a esta actividad son cada vez mayores. Por eso, la Amazonia Azul es un flanco muy importante para los intereses de Brasil.

Recientemente, sometimos un reclamo ante la Organización de las Naciones Unidas sobre nuestro deseo de ejecutar

la elevación de Rio Grande, que es una zona ubicada a 1400 kilómetros de la costa brasileña y que representa la extensión de la plataforma continental del país. A propósito, en el ámbito del Derecho fuimos capaces de demostrar los términos reivindicativos de esta área, ante la Organización Marítima Internacional. Esta acción es de suma importancia debido a que apostamos por el futuro del país; tenemos la plena seguridad que, de aquí a cien años, cuando la explotación del fondo del mar esté más adelantada, la elevación de Rio Grande será defendida por Brasil.

Debido a que el Atlántico Sur es punto clave para el comercio y exportaciones brasileñas, la defensa de nuestras líneas de comunicación —entendiendo la posición estratégica de Brasil en el océano— velan por que estas sean lo suficientemente extensas, al ser un área de tráfico de grandes buques cargueros y petroleros que transportan productos como la soya, alimentos y todo tipo de contenedores.

El sector político de Brasil estableció, como estrategia nacional de defensa, que el país deberá poseer una fuerza de submarinos convencional y de propulsión nuclear. Por tanto, es nuestro deber desarrollar dicha capacidad y proyectar su construcción a la brevedad; en tal sentido, destinamos todos los esfuerzos necesarios para el fortalecimiento del Prosub. Los trabajos iniciaron en el año 2008, bajo el acuerdo estratégico entre Brasil y Francia, luego firmamos siete contratos en el año 2009 más el inicio de la construcción de la primera unidad fabril en Itagüí en Rio Grande do Sul, su inauguración y, a finales del año pasado, el lanzamiento del submarino Riachuelo.

El Prosub está compuesto por tres grandes iniciativas que marchan en paralelo. Hoy en día, contamos con la infraestructura pertinente para la ejecución de las obras que, una vez potenciadas, darán comienzo a la producción de los submarinos. Asimismo, la construcción de los

cuatro submarinos convencionales está encaminada, habiéndose lanzado el primero durante el 2018, mientras que la unidad de propulsión nuclear se encuentra en fase de planificación.

Los pilares del Prosub fueron establecidos en la década pasada, siendo uno de estos la transferencia tecnológica. Hubo mucha gente que no creyó en este proyecto, sin embargo, tras diez años de trabajo tesonero, el objetivo fue conseguido. Asimismo, muchos sostuvieron que era imposible transferir tecnología en el área nuclear; en tal escenario, concluimos dejar de lado el tema y dirigir los esfuerzos hacia la transferencia de tecnología para la construcción de submarinos. Otro pilar del programa es la nacionalización del equipamiento y los sistemas, así como el adiestramiento del personal a cargo del programa como técnicos, ingenieros y militares —este último cimiento es el más importante—. Por otro lado, es preciso resaltar que estas bases propulsan la producción en la economía brasileña, tanto en el área tecnológica como en el campo de la construcción; estos sectores presentan avances tecnológicos y económicos muy significativos, por lo que esperamos que dichas mejoras continúen en los próximos años.

Un ejemplo de transferencia tecnológica ocurrió en el año 2010, cuando enviamos a Francia algunos operarios, ingenieros y técnicos. Ellos iniciaron la construcción de los submarinos convencionales y elaboraron la proa en la comunidad francesa de Cherbourg; dicho personal regresó a Brasil y generó el efecto multiplicador de sus conocimientos hacia centenas de operarios. Por otro lado, en el año 2013, se dio inicio a la construcción del casco resistente, mientras que en el 2017 esta infraestructura quedó lista para ser anexada a otras piezas en Brasil. Otro ejemplo de transferencia fue la creación del Centro de Desarrollo de Submarinos (CDS), el cual inició operaciones en Francia con treinta ingenieros, lo que significó un gran

aprendizaje en cuanto a la proyección de submarinos (en Brasil ya se habían construido algunos en la década del 90, pero la proyección de los mismos representó un proceso totalmente innovador).

En la actualidad, contamos con 200 ingenieros inmersos en la construcción de submarinos. Si bien es una cantidad interesante, nuestra meta es contar con 600 operarios entre ingenieros y técnicos; en ese sentido, venimos desarrollando un proceso dinámico, ya que las personas que trabajan en el área de proyectos se desenvuelven también en los departamentos de informática, estructura, balance térmico, balance eléctrico, balance de propulsión, requisitos de seguridad, sistema de combate —que desde mi punto de vista es el área más importante y nuestra mayor conquista—, el área de proyectos y en apoyo logístico integral. Fruto de este esfuerzo fue la construcción del submarino convencional SBR. El primero de ellos se llama Riachuelo y cuenta con cinco metros de longitud adicional, a diferencia de los submarinos Scorpene, de origen francés. Esta proyección fue concebida por los creadores brasileños y se hizo patente durante la construcción de la primera unidad. Hoy en día, se realizan prácticas y pruebas en puerto con dicha maquinaria.

Hablamos también de la nacionalización de la infraestructura industrial y naval como uno de los pilares del Programa de Submarinos. Pues bien, cerca de 700 empresas brasileñas colaboraron en la construcción del complejo de Itagüí en el aspecto material e industrial; estas compañías desarrollaron equipos que nunca habían sido fabricados en Brasil, especialmente en el área tecnológica. En la actualidad, tenemos más de cien proyectos nacionalizados y vinculados al sistema de submarinos convencionales, así como varias piezas, equipos y repuestos fabricados en el país; los motores eléctricos son hechos en Brasil, mientras que las válvulas de los cascos de los submarinos, tanto del modelo convencional como el de propulsión nuclear,

también son construidas en suelo nacional, contando además con diversas baterías y elementos necesarios para concretar los proyectos.

Esto facilita nuestra logística y permite que las empresas ingresen al mercado mundial para vender sus producciones a países que cuenten con programas de construcción de submarinos. En cuanto al entrenamiento del personal, tenemos instalados en Itagüí siete simuladores operativos y seis de ellos cuentan con tecnología brasileña. En tal sentido, las dotaciones de los submarinos convencionales Riachuelo y Humaitá vienen entrenando en base a estos sistemas.

La estrategia lanzada desde la década pasada para el éxito del Prosub fue la creación de una empresa civil. Nuestro astillero, llamado Itagüí Construcciones Navales, cuenta con casi 2800 empleados; si existiesen otros proyectos en el astillero, podríamos albergar hasta 5000 empleados en los diferentes sistemas. La infraestructura industrial fue el primer gran proyecto de las tres iniciativas y comenzó en el año 2010. Asimismo, fuimos eficientes en cuanto a la implementación de las instalaciones, pues lo hicimos a partir de un terreno vacío y tardamos exactamente dos años y cuatro meses en culminar los trabajos y poner en marcha las operaciones de la Unidad de Fabricación de Estructuras Metálicas (UFEM). Esta unidad recibe los equipamientos dentro del casco resistente (podemos apreciar en imágenes los submarinos dentro de la UFEM) y, en otra unidad del astillero, en

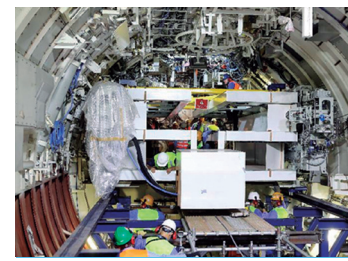


Imagen 1, 2 y 3: La Unidad de fabricación de Estructuras metálicas, con 98 mil metros^2 y 45 edificaciones.
Fuente: expuesto por el autor.

una isla cercana a la UFEM, levantamos la unidad final, que es otro astillero de construcción, en una isla anteriormente considerada como un área degradada. La Marina ejecutó trabajos de limpieza y reconstrucción en dicho lugar, lo que facilitó la confección de un astillero en el mar. Cabe mencionar que estas instalaciones fungen de base naval y astillero a la vez, contando con 651 mil metros cuadrados de área total y 92 edificios. En el futuro, planeamos construir el astillero de apoyo para la construcción del submarino de propulsión nuclear.

En diciembre del 2018, lanzamos el submarino Riachuelo, el cual se encuentra en el mar realizando pruebas. Estas actividades anuncian que el futuro del Prosub se aproxima con cada año que pasa: en el 2019 lanzaremos el submarino Humaitá, en el año 2021 el submarino Tonelero y en el 2022 el Angostura. Recordemos también que Itagüí se ubica estratégicamente en el estado de Río de Janeiro, a 70 km de la ciudad en la bahía de Sepetiba. En dicho sector contamos con tres grandes unidades de fabricación: la Nuclep, la UFEM y un astillero de construcción.

La Nuclep es una empresa oriunda que nació del proyecto de energía nuclear y que terminó convirtiéndose en un programa de tecnología nuclear forjado junto con Alemania en la década del 70. Asimismo, fue constituida en base a dos pilares nucleares, siendo uno de ellos la industria de mecánica pesada, la cual está instalada desde la década del 80 y sirve para construir los cascos resistentes de los submarinos; dentro de

Imagen 4 y 5 : NUCLEP, prensa hidráulica de 80.000 kn
Fuente: expuesto por el autor.

Imagen 6 : gran mecanizado.
Fuente: expuesto por el autor.

Imagen 7 : calandrias y prensas.
Fuente: expuesto por el autor.

Imagen 8 : máquina de corte por hidrojet.
Fuente: expuesto por el autor.

ella tenemos una prensa hidráulica de ocho mil toneladas, que ha servido para la conformación de la proa del casco resistente. Esta es una capacidad que no poseíamos en el ochenta, periodo en el que se construyeron los submarinos de origen alemán; hoy en día, esta prensa es una de las más grandes en el hemisferio sur y es capaz de trabajar en los submarinos de propulsión nuclear.

En la Nuclep se concibió la fabricación del casco de presión, en base a trabajos de mecánica pesada, con el fin de ejecutar cortes en las chapas, la calandra, la unión de soldaduras de las chapas de subsección, en la unión de la subsección y la sección.

Cuando esto quede listo, los trabajos pasarán a las instalaciones de la UFEM, donde los equipos serán rellenados. La UFEM (ubicada al lado de la Nuclep) posee un edifico principal en cuyo interior están colocados dos submarinos que serán equipados y sistematizados con una facilidad nunca antes vista en otros astilleros.

Estas secciones cuentan con tanques internos y el equipamiento necesario para el armado de los submarinos dentro del casco resistente, considerando además el tratamiento acústico y la prevención de ruidos, con la finalidad de que sean silenciosos. Otro ejemplo importante son los bancos de los motores eléctricos y diésel, ya

que los submarinos poseen un motor eléctrico de bajo consumo y alto desarrollo.

Al lado del edificio principal de la UFEM contamos con importantes talleres de fabricación de estructuras no resistentes, carpintería y aislamiento, las cuales ofrecen los equipos que serán instalados dentro de los submarinos. Además, se cuenta también con un sistema Soft Patch que permite prescindir de la ejecución de cortes al casco para retirar las máquinas y motores eléctricos. A su vez, tenemos un taller de tuberías digitalizadas y con máquinas numéricas elaboradas por computadora para tuberías de diámetros grandes.

Las secciones son trasladadas para ser armadas en otro astillero pasando por una carretera, luego por un túnel y por las instalaciones de nuestra Marina, llegando finalmente al astillero de construcción para la integración de secciones, acabados y pruebas. Precisamente, aquí teníamos dos submarinos: uno ya se encuentra en el agua y el otro al interior del edificio; como podrán observar, en el lado derecho apreciamos como quedará la construcción de los tres astilleros en los que construiremos nuestro submarino nuclear y recibiremos hasta cinco submarinos al mismo tiempo.

Imagen 9 : UFEM, fabricación de estruturas no resistentes, pre-equipamiento y equipamiento.
Fuente: expuesta por el autor.

Por otro lado, el astillero de construcción comenzó sus operaciones en el año 2018, con la transferencia del primer submarino. Si bien las secciones fueron integradas y soldadas minuciosamente, permítanme apuntar que existe algo más difícil que la construcción del submarino y la instalación de tuberías: me refiero a la integración de sus sistemas. Estos deben colocarse a la perfección, ya que un desperfecto en el proceso generaría problemas en las pruebas del submarino. Por tal motivo, este astillero cuenta con la capacidad de integrar sistemas eléctricos y mecánicos, tras el término del proceso de soldadura del submarino.

De igual modo, tenemos un edificio y un taller principal de fabricación de submarinos en los que son integradas y unidas las secciones, contando para ello con dos grandes grúas de 150 toneladas de capacidad que permiten mover grandes piezas. Una vez que el submarino queda listo es transportado por medio de un sistema de rieles. Aquí podemos apreciar a los submarinos Humaitá y Riachuelo dentro del taller.

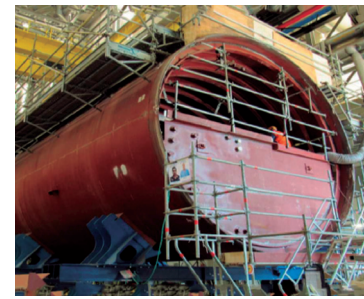


Imagen 10 y 11 : talleres de montaje de las secciones y de pre-equipamiento. Instalación de tanques internos.
Fuente: expuesto por el autor.

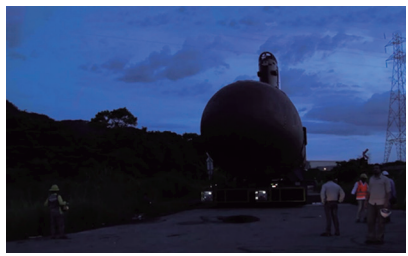


Imagen 12y 13: UFEM, transporte UFEM-ESC.
Fuente: expuesto por el autor.

Imagen 14: las secciones son trasladadas, para ser armadas a otro astillero.
Fuente: expuesto por el autor.

Por otra parte, contamos con talleres auxiliares que poseen una taladradora de apoyo para la construcción de submarinos. En tanto, tenemos los talleres de electromecánica, donde se realiza el mecanizado del Soft Patch; además, contamos con taladros para la fabricación de piezas de los submarinos, hecho que nos permite prescindir de la industria civil. En ese sentido, contamos con un edificio de apoyo a la fabricación donde funcionan talleres de pinturas y de activación de baterías automatizadas. Cabe resaltar que este es un proyecto de sello brasileño, el cual se espera sea ejecutado de forma controlada, para que las baterías prolongadas tengan una vida útil. Como bien saben los camaradas submarinistas, esta es una cuestión importante para los submarinos.

Finalmente, contamos con el elevador de buques en la punta del astillero, el cual posee una capacidad de ocho mil toneladas, 110 metros de extensión y 20 metros de ancho. Esta estructura fue pensada para la recepción del submarino de propulsión nuclear. Asimismo, es totalmente automatizado y compuesto por 34 grúas que han sido operadas varias veces.

En relación al submarino nuclear, deseamos construirlo tanto en la parte mecánica como en la de inmersión. Dicha estructura es muy compleja en cuanto a su construcción, por lo que representa un verdadero reto para el ser humano ingresar a su unidad mecánica, en lo referido a la colocación de las piezas y la cantidad de operarios que se necesita para construirlo. El proyecto básico del submarino nuclear brasilero terminó en el año 2017 y fue declarado accesible tanto por Brasil y Francia, en cuyo país fungimos como autoridades del proyecto y los franceses como asesores.

Hasta el año 2021 llevaremos a cabo las negociaciones del contrato. Es necesario mencionar que el Prosub está construyendo la proa y parte de la popa del submarino nuclear. Por otro lado, si bien el reactor será fabricado por brasileros, dicha iniciativa no forma parte del Programa de Submarinos, debido a que es parte del programa nuclear de la Marina. Es evidente que nos desplazamos por cuerdas separadas, sin embargo, estamos integrados de alguna forma con ellos, ya que serán los encargados de construir la sección del reactor nuclear sin ninguna participación extranjera.

Imagen 15: 2 grúas aéreas rolantes con capacidad de 150 toneladas y otras 2 de 30 toneladas.
Fuente: expuesto por el autor.

A su vez, Brasil negociará los contratos mientras culmina la construcción del prototipo del reactor lLabegne, el cual será utilizado en los submarinos y que se encuentra en Sao Paulo sometido a labores de fiscalización. Su propulsión actúa como si fuera un submarino, pero en un ambiente más controlado. Una vez estabilizado, se procederá a instalarlo dentro del submarino. En ese sentido, esperamos la culminación del prototipo para iniciar la construcción del submarino, lo cual estimamos sucederá en el año 2021.

Imagen 16: submarinos Riachuelo y Humaitá.
Fuente: expuesto por el autor.

sesión

2.1

El sigilio en las unidades submarinas

Dr.
Roger Berg

La compañía SAAB Kockums ha diseñado y construido submarinos por más de cien años. En tal sentido, nuestro primer contrato data de 1914, generándose luego una producción en serie de nuevas clases; por ello, hemos diseñado y construido diferentes clases de submarinos, en un periodo que fluctúa entre los diez y quince años, mayormente para la Marina Real Sueca, incluyendo también contratos de exportación. Cabe mencionar que nosotros somos los diseñadores de los submarinos de Australia clase Collins y de algunos destinados hacia Singapur.

Asimismo, el submarino clase Gotland es el que opera actualmente en la Marina Real de Suecia y, a su vez, pusimos en marcha un proyecto para modernizarlos; la última unidad fue lanzada este verano y se encuentra en fase de prueba, mientras le añadimos nuevas capacidades, nuevos sensores y mejoras en su desempeño. En base a ello, por ejemplo, integramos un nuevo sistema de propulsión independiente y efectuamos mejoras en el sigilo.

Este submarino fue proyectado para probar los conceptos de la nueva unidad diseñada para la Marina Real de Suecia: el A26 o el clase Blekinge. Es preciso que sepan que muchos de los sistemas implementados en este submarino serán utilizados en otras unidades y serán probados durante la etapa de modernización. A estos nuevos submarinos se les llamó Blekinge Class-A26; sé que es una palabra bastante complicada, pero se determinó la clase de estos submarinos acorde a los diferentes condados de Suecia y a la ubicación de la Base Naval y el astillero. Aparte de ello, déjenme decirles que es el rey de Suecia el que decide los nombres. Este submarino de nueva generación está diseñado para operaciones litorales y oceánicas.

Anteriormente, nuestras unidades enfocaban las acciones en el Mar Báltico, siendo la misión principal detener una posible invasión rusa. Sin embargo, el mundo ha cambiado

y ahora se requiere cumplir nuevas tareas y operaciones por parte de los submarinos, lo que significa que estos deberán ser mejorados en cuanto a sus capacidades en el océano, como es el caso del sigilo en las unidades. Si hablamos de ello, nos referimos a un submarino de nueva generación y con gran autonomía, en base al uso del sistema independiente de propulsión de aire Stirling, de baja firma acústica.

No obstante, una de las características clave en este tipo de unidades es la alta resistencia al impacto, la cual es comprobada mediante pruebas realizadas a escala completa, como el caso de los primeros submarinos de las nuevas clases suecas, que pasan por pruebas muy severas de impacto. Por supuesto, le añadimos también nuevos sensores e introdujimos el concepto flexible de carga, lo que significa que, en el futuro, podremos añadir nuevas características a los submarinos.

Figura 1: El módulo Stirling Mk III que opera en la Armada de Suecia y también en algunos submarinos de exportación (izquierda). El nuevo modelo Stirling Mk IV es desarrollado en el programa (derecha). Fuente: expuesto por el autor.

Uno de los nuevos sistemas introducidos es el Payload Lock Flexible, que es un tubo grande de 1,5 metros de diámetro y 6 metros de largo, colocado en la parte frontal; es considerado como un sistema “multimisión”, que puede ser utilizado para llevar a cabo diferentes tareas como el transporte de equipos de operaciones especiales, o vehículos autónomos, y el despliegue de sensores.

Ahora bien, cuando nos referimos al sigilo hablamos del arte de no ser detectado, además de ser una función que posee varios parámetros. Una de ellas es, por ejemplo, el manejo de la firma acústica, lo cual refiriere a la mínima emisión de sonido. Sin embargo, esto no es lo único, pues también se debe monitorear y mantener baja la propia firma acústica, tarea que implica medir el submarino para sostener una baja emisión acústica, sumada a las nuevas tecnologías como la propulsión independiente de aire, que ofrece nuevas capacidades junto con el sigilo. Finalmente, tenemos el comportamiento operacional, factor de vital importancia para la obtención del sigilo.

Y ya que hablamos sobre tecnología, nos referiremos a la capacidad del submarino de mantenerse sumergido, debido a que es la principal propiedad del sigilo. Como dato adicional, sepan que las nuevas tecnologías han permitido incrementar el tiempo de inmersión de las unidades. En esa línea, el primer submarino de madera que tuvimos, hace cientos de años atrás, solo podía permanecer sumergido una cuantas horas; luego pasamos a los submarinos convencionales, los cuales se mantenían inmersos por unos cuantos días. Hoy en día, a través del sistema de propulsión independiente de aire, un submarino puede mantenerse sumergido por semanas. En el caso de los submarinos nucleares, nos encontramos frente a unidades particulares, ya que poseen la capacidad de permanecer sumergidos por tiempo indefinido y la única limitación es la comida que debe llevarse a bordo para la tripulación.

Actualmente, las unidades trabajan en base a una propulsión independiente de aire basada en la tecnología Stirling. Aquellos que han leído sobre física, seguro conocen el motor Stirling, el cual trabaja en base al calor, lo que significa que tiene un gas trabajando en frío a un lado del pistón. Esto genera la diferencia en la presión, haciendo que los pistones se muevan y generen electricidad.

Esta combustión de calor continuo lo vuelve silencioso y aumenta la autonomía de inmersión dramáticamente.

La unidad puede funcionar con diferentes combustibles y es necesaria la utilización de oxígeno líquido, con el fin de que sea quemado en la cámara superior, mientras se recolectan ondas de calor en el sistema superior, para luego transferirlo a la parte de arriba de los pistones. Cuando estos cuatro pistones se encuentren conectados, tendremos como resultado un motor V4. En la parte inferior pueden apreciar que es semejante a un motor ordinario, pues tiene cierto balance para mantener un sonido muy bajo.

Por otra parte, las ventajas que se buscan obtener con este sistema es el aumento de la autonomía de inmersión y la obtención de una alta eficiencia de acción. Hoy en día estamos trabajando en la implementación de un sistema de recuperación del calor excedente, el cual será utilizado para otra estructura, con el objetivo de calentar el agua y depurar el aire, de manera que podremos regenerar el dióxido de carbono que capturamos en el sistema.

Precisamente, este sistema tiene muy baja vibración, por lo que una persona podría estar tranquilamente al costado de esta, cuando se encuentre funcionando a toda potencia. Es importante resaltar que no tiene firma infrarroja, debido a que enfriamos los gases de escape dentro de agua refrigerada y el dióxido de carbono se disuelve fácilmente en ella. Este sistema lo usamos desde 1989 y, al día de hoy, es utilizado por todos los submarinos de Suecia y por otras marinas.

Entre sus atributos, destaca su alta disponibilidad y confiabilidad, el bajo costo de su ciclo de vida y el práctico mantenimiento que ofrece. Sobre este último punto, puede ser desempeñado por los propios miembros de la tripulación, ya que es similar a un motor diésel estándar y es muy fácil de recargar (en base a cuotas de hidrogeno

líquido y combustible). Este hecho ha sido demostrado por la Marina Real de Suecia, en muchos ejercicios internacionales.

Del mismo modo, hemos reacondicionado submarinos en base a este sistema, diseñando una sección de peso neutro, el cual contiene toda la estructura y que puede ser colocado en un submarino antiguo. Permítanme decirles que nosotros contamos también con un desarrollo tecnológico propio, el cual viene desde la década del setenta, periodo en el que se realizó mucha investigación sobre sistemas como el diésel, diésel de ciclo cerrado, sistemas cerrados de turbinas, celdas de combustible y también los de propulsión nuclear. Posteriormente, a inicios de los ochenta, decidimos ir un poco más allá de los sistemas Stirling, los cuales fueron probados en puerto mediante una sección construida; debido al éxito obtenido en los testeos, se decidió reacondicionar el submarino HMS Nacken con una sección completa del sistema Stirling abordo y, un año después, se dispuso que el submarino Gotland Class también fuese equipado con dicho sistema, lo que devino en el desarrollo de la versión MK II y cuya licencia fue exportada a Japón. En la actualidad estamos trabajando en el MK IV clase A26, el

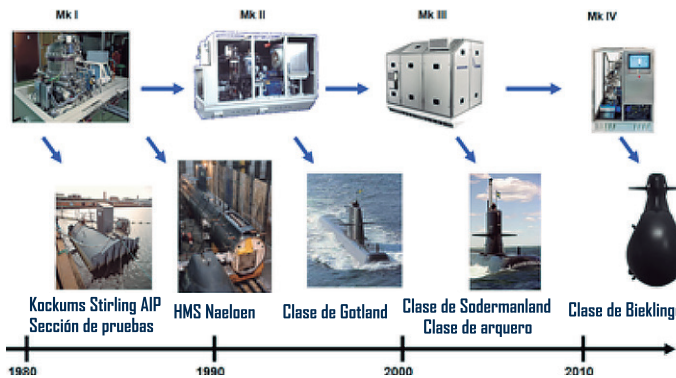


Figura 2: el desarrollo evolutivo del sistema Stirling AIP.
Fuente: expuesto por el autor.

cual es un nuevo sistema y más pequeño que su antecesor (la mitad del tamaño del MK II) y, como les mencioné, en esta versión también incluiremos la recuperación del calor y la optimización, para mejorar la eficiencia del sistema. Por otro lado, buscamos añadir manufactura por adición, como la impresión 3D, para conseguir los componentes del motor.

La siguiente parte es la gestión firmas. En mi opinión, creo que tenemos submarinos con muy bajas firmas y, en ese sentido, contamos con la gran cooperación de la Marina de Suecia, lo que significa el acceso a data del campo de hidrófonos. En tanto, es importante obtener el feedback correspondiente respecto al funcionamiento del sistema, cómo son las firmas del mismo y los puntos que deben recibir mantenimiento y mejoras. Somos conscientes, además, que debemos tener capacidades de modelamiento avanzadas, con el fin de hacer una predicción respecto a cómo serán estas firmas y la forma de reducirlas.

Para ello, contamos con un excelente proceso de gestión de firmas y una visión holística. Por otra parte, tenemos capacidades de análisis y medición de los diferentes tipos de rastros; como podrán ver, en la parte inferior del gráfico, el rastro más típico es el ruido irradiado, sin embargo, contamos también con rastros magnéticos, hidrodinámicos, fuerza del blanco (que es una característica acústica) y rastros eléctricos. En tal caso, si necesitásemos izar mástiles o sacar la vela en la superficie, tenemos a disposición el rastro infrarrojo y el radar Cross Section.

Respecto al ruido radiado, hay diferentes efectos que lo producen. El más común es el generado por las máquinas rotatorias, las cuales crean ruidos de banda ancha, que pueden ser transferidas fuera del agua y a los sistemas de fluidos abordo. Por otro lado, existen también diferentes ruidos de flujo, como los flujos externos, cuando el submarino se desplaza, y también los flujos abordo, los cuales manejamos cada uno de

nosotros (ruidos provenientes de los ductos de ventilación, tuberías de enfriamiento, entre otros). Asimismo, hay otra clase de ruidos llamados transitorios, que son aquellos que se elevan durante ciertos tiempos, como al abrir escotillas o izar mástiles. Finalmente, debemos tomar en cuenta también el propio ruido del sonar.

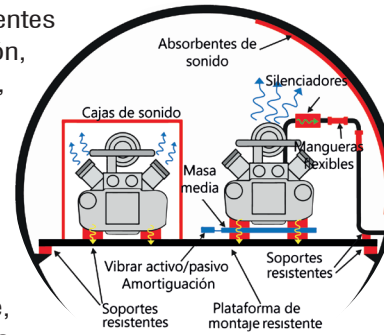


Figura 3: los principios generales de reducción del ruido para el ruido de la estructura (flechas amarillas), el ruido fluido (flechas verdes) y el ruido aéreo (flechas azules). Fuente: expuesta por el autor.

No obstante, hemos tomado diferentes medidas en cuanto a la reducción del ruido. Una de las más importantes es la utilización de un diseño de plataforma resilente con compensadores, mangueras y cables flexibles; del mismo modo, tenemos que trabajar en base al diseño de la hélice, ya que es una parte muy importante a tomar en cuenta, cuando se intenta reducir los niveles de ruido. En ese sentido, se necesita de amortiguadores que eviten las resonancias de la misma.

El diseño de la plataforma silente que utilizamos es muy adecuada, debido a que la mayoría de sistemas han sido instalados de antemano, lo que significa que hemos simplificado este proceso, para avocarnos en la fase de pruebas de los sistemas. Cabe mencionarles que todo esto se ejecuta antes de cerrar el casco ya que, una vez sellado, todo se vuelve más complicado, al contar con pequeñas escotillas y con menos espacio para realizar maniobras y pruebas.

Esta plataforma resilente se asienta sobre elementos de jebe, para absorber vibraciones y, de esta manera, reducir los ruidos de la maquinaria y los transitorios, así como también los requerimientos de choque de algunos componentes. Esto forma parte de nuestro diseño modular

en Sabb Kockums, el cual diseñamos de este modo para que la construcción sea más fácil y prepararla para futuras actualizaciones (por ejemplo, si decidiésemos cortar el casco para hacerlo más grande, añadir el modulo y elaborar diseños personalizados para nuestros clientes). El concepto del diseño de este modelo evidencia nuestra preparación para las modificaciones futuras y la adaptación eficaz a los requerimientos de los clientes.

De este modo, colocamos los módulos Stirling y los de las máquinas diésel. Sobre este último, hemos desarrollado módulos de diésel basados en la experiencia de los de clase Stirling; estos son auto contenidos por las máquinas que generan la protección contra incendios, el aislamiento y acciones anti shock. En la parte inferior tenemos una sala de maquinaria auxiliar colgada, la cual permite aislar, de mejor manera, diferentes tipos de compresores y bombas de la estructura del casco. Al ser una plataforma muy grande, uno de los retos es montarla dentro del casco del submarino.

Anteriormente mencioné que es importante medir y mantener las emisiones, pues bien, en Suecia efectuamos mediciones acústicas una vez al año. Una de las formas en que llevamos a cabo este proceso es en base a la medición estática, en la que el submarino queda colgando, sostenido por las boyas, para que podamos activar uno a uno los sistemas; luego medimos el nivel de ruido radiado por diferente lados y a distintas distancias, con el fin de testear cada sistema. Por ejemplo, si tuviésemos un problema en el sistema hidráulico, este puede ser aislado y medido.

Asimismo, contamos con un campo dinámico. Esto quiere decir que el submarino pasa por un track, con el fin de operar en diferentes condiciones y velocidades y, posteriormente, pasará por el snorkel para la medición del ruido. Por lo general, este tipo de mediciones son efectuadas por la Marina de Suecia, pero en SAAB Kockums también las ejecutamos con fines comerciales y por requerimiento

de nuestros clientes (de hecho, algunos han pedido el desarrollo de estos campos de medición).

La siguiente característica es la fuerza del blanco, que es la propiedad acústica de reflexión del submarino. En ese sentido, sabemos que es muy difícil detectar a un submarino con el sónar pasivo, por lo que la importancia de la fuerza del blanco se ha incrementado. La amenaza a la que nos enfrentamos es muy amplia, ya que tenemos que trabajar con frecuencias que van desde 1 a 2 Kilohertz de los sonares remolcados, hasta torpedos con homming acústico, que van de 25 a 75 Kilohertz, lo que representa un rango acústico muy grande. En tanto, el diseño basado en la fuerza del blanco acústico necesita de un modelamiento capaz de predecir los distintos reflejos acústicos.

Otro punto a tomar en cuenta es la influencia del entorno operacional requerido. Como ustedes saben, la velocidad de propagación del sonido tiene un perfil y el rebote en el fondo influenciará en el campo acústico directo del submarino. Esto quiere decir que, en el mejor de los casos, se contará con un perfil de impacto, pero la realidad es que el campo acústico provendrá de diferentes direcciones, dependiendo del entorno operacional. En tanto, la naturaleza del campo acústico influenciará en el diseño geométrico del submarino.

Entre otras cuestiones, realizamos una serie de análisis estadísticos en diferentes ambientes operativos de nuestros clientes y, de acuerdo al lugar en el que operaban, fue posible visualizar cuales serían los diferentes campos acústicos de un submarino. A su vez, contamos con diferentes herramientas para realizar este trabajo, en el cual podemos simular un submarino, incluyendo todos los detalles e incluso el ambiente acústico; es posible aplicar también diferentes propiedades de materiales, acciones de transmisión y reflexión, así como la visualización de los efectos de dispersión de volúmenes de agua, producto de una inundación, tal como se tiene en la parte trasera y en la proa.

Como ustedes sabrán, si tenemos un material como el acero y el agua en ambos lados, los elementos que se encuentren dentro de la carcasa tendrán una gran dispersión del ruido. Por ello, se necesita aplicar lo que se conoce como “recubrimiento de pérdida por transmisión”, el cual no absorbe la energía, sino que la dispersa en la dirección correcta. De la misma forma, podemos analizar la modelación, la monoestática o la biestática. Sobre este punto, hablamos de monoestática cuando se envía y recibe en la misma posición, mientras que la biestática refiere a posiciones diferentes, que pueden ser verificadas con varias mediciones. Existen muy pocos países en el mundo que cuenten con campos completos de medición para la fuerza del blanco, como el caso de Suecia, por lo que resulta necesario ejecutar la tarea de modelación.

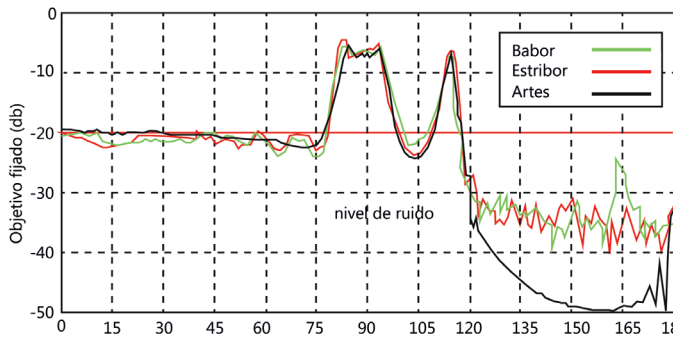


Figura 4: medido (rojo y verde) y calculado (negro). El TS para un modelo de submarino (cilindro equipado con estera de casco y cono de popa). El nivel de ruido también está indicado (azul).
Fuente: expuesto por el autor.

Vistos estos conceptos, cabría preguntarse entonces cómo se visualiza esta fuerza del blanco acústico. Lo que aprecian en la parte superior es lo que van a encontrar en un submarino genérico. La línea azul representa el TS, en función al ángulo de incidencia en la composición mono estática. Asimismo, tenemos diferentes efectos en la proa: tenemos el médium TS, marcado con el arco ancho de color rojo. Por otro lado, la parte trasera alta del TS se

ubica en un sector mediano, mientras que en las bandas se tiene el casco resistente y por eso es muy alto y colocado en un sector pequeño. Finalmente, está el cono trasero alto TS, pero en un pequeño sector.

Este tipo de análisis, junto con el estudio del ambiente operacional, nos permite tener diferentes diseños geométricos, como por ejemplo, la aleta del submarino, que pueden ver en la parte inferior, tiene una forma parecida al Stealth y se elaboró en base a un análisis que hicimos. Esta es una buena forma de reconocer submarinos; en la parte inferior izquierda verán a Tom Holland, quien fue el diseñador del primer submarino moderno y, tal como se aprecia, todos los diseñadores han seleccionado diferentes modelos de aletas. En realidad, no solo importa el TS, sino también la hidrodinámica y eso dependerá de la velocidad con la que fue diseñada. Por ejemplo, si se diseñase un submarino nuclear, se requiere que este cuente con una mayor velocidad que el submarino convencional, hecho que tendrá una gran influencia en su diseño.

Entonces, las medidas que hemos tomado para reducir el target strength, en este nuevo submarino, son las formas geométricas de los planos, pero también del casco; luego, seleccionaremos los materiales correctos. Estos submarinos fueron equipados con coberturas de pérdida de transmisión, para prevenir cualquier ingreso de ondas acústicas, en áreas inundadas, así como también se añadió un revestimiento acústico anecoico (este material es producido por el Instituto Nacional de Defensa, siendo la forma en la que nosotros conseguimos suministros).

Además, contamos con un conformal array, que es un arreglo que sigue la forma del submarino. En tanto, al no poseer una ventana acústica muy grande, que cubra el arreglo cilíndrico, se evitará la filtración de sonidos hacia la estructura interna del submarino, lo que simplifica su diseño, al tener diferentes tanques, en lugar de una unidad cilíndrica.

Ahora, pasemos a hablar sobre los rastros no acústicos. Tenemos muchas amenazas que intentan localizar a los submarinos, utilizando precisamente este tipo de rastros (siendo las minas las más conocidas). Sin embargo, en la actualidad se utilizan también los rastros eléctricos, referido a la detección magnética y a los diferentes sensores utilizados en los aviones de patrullaje marítimo. Por otro lado, tenemos el SQUID y los sensores multi-influencia y los de tipo eléctrico.

Por otra parte, están los rastros galvánicos eléctricos, ya que no estamos únicamente frente a una cuestión eléctrica, sino también magnética. Este rastro es generado por diferentes metales unidos al agua y con conductividad eléctrica, lo que origina corrientes de corrosión, que pueden ser detectadas a distancia. Existen diferentes tipos, como la estática y la dinámica. Para ejemplificarlos, sucede que, cuando tenemos una hélice, en lo que llamamos el ELFE (Extreme Low Frecuency Electric), los rastros eléctricos que genera crean, a su vez, rastros magnéticos que, como ustedes saben, si tenemos una corriente eléctrica generará un campo magnético. Por tanto, debemos ser capaces de modelar este tipo de rastros para reducirlos, utilizando técnicas pasivas, es decir, evitar que ocurran estas corrientes, colocar los ánodos de sacrificio en el submarino y prevenir estas ocurrencias, mediante el uso de pinturas anticorrosivas (que cómo ustedes saben, evitan la corrosión y el óxido).

En tanto, también hay técnicas activas como la ICCP (Impressed Current Cathodic Protection), la cual es común en el ámbito civil, en cuanto a la detección de la corrosión a través de electrodos, en vez de la utilización de ánodos de sacrificio. En tal modo, es posible utilizarlo para reducir su rastro galvánico, así como también mediante un sistema que conecta el eje a tierra y trata de reducir las corrientes que van desde el casco hacia la hélice.

Finalmente, tenemos al rastro magnético, el cual es producido por diversos efectos. El más obvio es la magnetización inducida, la cual se da cuando una parte ferro-magnética es movida dentro de un campo magnético, lo que genera un proceso de magnetización en sí mismo. Por otro lado, están los momentos magnéticos permanentes, dentro de la parte ferro-magnética, que convierten a la unidad en un imán. Esto puede reducirse mediante el uso del sistema de degaussing. Cada vez que un submarino es sumergido, se produce un cambio en el magnetismo del casco, produciéndose la inserción de momentos magnéticos permanentes.

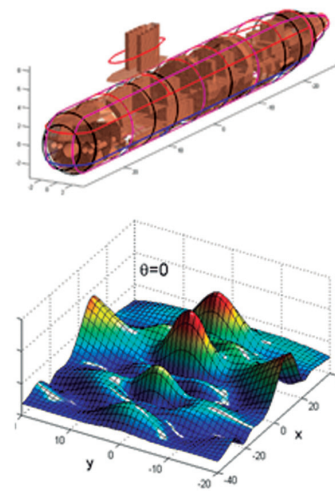


Figura 6: ejemplo de modelo, con bobinas de corriente, para el modelado de armadura magnética (izquierda) y la armadura magnética obtenida a una distancia determinada por debajo del submarino (derecha).
Fuente: expuesto por el autor.

Todo esto se reduce con un sistema avanzado de degaussing, con bobinas en los tres ejes y en el hecho de determinar cuanta corriente es necesaria para cada bobina, con el fin de contrarrestar el magnetismo de la tierra en ese momento. Esto se logra teniendo sensores externos de magnetismo o al usar un mapa magnético. En ese sentido, diseñamos un modelo utilizando la técnica del modelamiento de elementos finitos de rastros magnéticos, para elaborar el sistema de desmagnetización, determinándose cuantas bobinas debe haber y la localización precisa de las mismas. Dicho sea de paso, un sistema moderno de degaussing puede reducir el magnetismo en más de un 90%.

Es muy importante mantener bajos los niveles de rastro y ser capaces de medir varios de estos fenómenos. Por ello, contamos con un centro de pruebas en la ciudad de Malmo, en el sur de Suecia, la cual es una instalación muy importante para el diseño de submarinos. Allí realizamos

diversas pruebas de ruido y vibración, así como pruebas magnéticas, de presión hiperbárica, y mediciones de estrés y tensión. Contamos con un tanque de presión de 30 metros de largo y 3 metros de diámetro, el cual puede ser presurizado hasta con 160 bares. Por lo general, lo utilizamos para las pruebas de soldadura; por otro lado, también hacemos mediciones de carga y choque y análisis de materiales, lo que evidencia que contamos con equipos para hacer pruebas a escala total del submarino.

A modo de conclusión, me permito decirles lo siguiente:

- El sigilo no solo se basa en el manejo de firmas, sino que es un tema ligado a la tecnología y a cuestiones operacionales, así como a mediciones y análisis constantes. Asimismo, significa mantenerse en inmersión, siendo la propulsión independiente de aire algo vital para esto.
- La gestión de rastros es una tarea multidisciplinaria, debido a que cubre una serie de tecnologías (física, mecánica, electrónica, electromagnética y química). Por ello, el enfoque debe ser holístico, en cuanto al manejo de firmas y rastros. Esto significa conocer todos los rastros y determinar cuál es el punto que podría generar una detección repentina.
- El modelamiento de predicción de todas las firmas también es requerido con suma importancia, así como la habilidad para medir y analizar los rastros. Por ello, se necesita entender el entorno operacional, ya que no se trata solo de aplicarlo para la fuerza del blanco acústico, sino para los diferentes tipos de ruido.

Creo que tenemos bastante experiencia en esta área, por lo que considero que somos capaces de diseñar y construir submarinos extremadamente sigilosos.

Referencias

A. Eriksson, *"Acoustic Target Strenght Design for Submarines – Modeling and Measurement"*, UDT-08, Glasgow, Reino Unido, 2008.

D. Nilsson, *"Next Generation Stirling AIP System"*, Maritime Systems and Technologies Europe, Yokohama. 2015.

G.H. Schneider, R. Berg, L. Gilroy, I. Karasalo, I. MacGillivray, M. Ter Morshuizen y A. Volker, "Acoustic Scattering from a Submarine: Results from a Benchmark Target Strength Simulation Workshop", 10° Congreso Internacional de Sonido y Vibración, Estocolmo, Suecia, Julio 2003.

H. Gustafsson, A. Eriksson, P-O Hedin y J. Jensen, *"State of the art CFD analysis for hydrodynamic design in submarine development"*, 11° Seminario sobre Tecnología de Plataformas Navales" Singapur, mayo 2007.

J. Frennberg, *"Submarine Section for Noise Measure"*, UDT-92, Londres (Reino Unido), junio de 1992.

J. Jensen, *"CFD in Submarine Design"*, Fluent UGM (User Group Meeting), Gotemburgo, Suecia. Octubre de 2003.

P. Granberg,*"Contributions of Permanent magnetic Moments to the Ferromagnetic Signature of a Submarine"*, EMSS03, Berlín, Alemania, junio 2003.

P. Granberg, *"Irreversbile Contributions to the Ferromagnetic Signature of a Submarine"*, UDT-03, Malmo, Suecia, junio 2003.

R. Berg, *"Stealth and Signature Management in Submarine Projects"*, Seminario sobre Tecnología de Plataformas Navales- Tecnología de Transformación para la future Marina. Singapur, mayo de 2005.

R. Berg, *"Signature Management and Stealth Design for AIP Submarines"*, UDT Pacific, Sydney, Australia, 2008.

R. Berg, *"Evolutionary Development of AIP Submarines"*, Defense Technology Symposium, Singapur, 2015.

R. Berg y H. Wicklander, *"Swedish AIP Submarine Development"*,

UDT Europa, Oslo, Noruega, 2016.

R. Berg, *"Applied Hydroacoustics in Submarine Design"*, Plataforma Naval – *"Trascending Technology Boundaries – Defining Tomorrow's Possiblity"* Singapur, mayo 2001.

R. Berg, *"Numerical Calculations of Acoustic Target Strenght – Environmnetal Influence"*, UDT-02, La Spezia, Italia, junio 2002.

S. Rikte, *"Formulation of the Signature problem of Galvanic Origin"*, UDT-03, Malmo, Suecia, junio 2003.

S. Rikte, *"Formulation of the Signature problem of Galvanic Origin"*, EMSS03, Berlín, Alemania, junio 2003.

R. Berg, *"Signature Management and Stealth Design for AIP Submarines"*, UDT Pacific, Sydney, Australia, 2008.

SESIÓN 2.2

Calm.
Javier
Bravo de Rueda

La construcción naval es un desarrollo industrial muy importante en la actualidad. Bien sabemos que este proceso no solo abarca los sistemas de cascos, de propulsión, los sistemas complementarios, las inversiones, puestos de trabajo y el tema socio económico. A esto se suma el diseño y la arquitectura naval, que con el tiempo han desarrollado grandes experiencias que permitieron modelar buques de diferentes tipos y características no solamente para las armadas, sino también para la marina mercante, la pesca, el transporte de pasajeros y la recreación, a través de la implementación y modernización de los sistemas de diseño y pruebas previas que permiten optimizar el proceso constructivo en los astilleros.

Esto generó, al interior de los astilleros, que la tarea del diseño pueda competir, desarrollarse y generar innovación. En ese sentido, estoy seguro que nuestros expositores nos mostrarán parte de esa importante información, referida a cómo se encuentra el alcance tecnológico y el avance de la construcción naval en el mundo.

Cabe precisar que la astillería en el mundo ocupa un espacio muy importante en las regiones, debido a que supone el desarrollo de proyectos conjuntos entre diferentes astilleros y armadas del mundo. El éxito de esta iniciativa dependerá de la apertura de las principales empresas en materia de la industria naval.

En primer lugar, contamos con la presencia del ingeniero Juan Carlos Díaz Cuadra, encargado de la Dirección Comercial y Desarrollo de Negocios de Navantia – España, quien disertará respecto a los nuevos escenarios de construcción naval y la transferencia tecnológica. Por otra parte, hará lo propio el ingeniero Paolo Tornese, representante de la entidad italiana Fincantieri S.p.A, quien comentará sobre la forma en que los aspectos de supervivencia impulsan el diseño de las naves de combate.

sesión

2.2

Nuevos escenarios de la construcción naval: transferencia de tecnología

Ing.
Juan Carlos
Díaz Cuadra

Somos conscientes de la evolución que estamos viviendo en los últimos años. El salto tecnológico, la avalancha digital y la globalización son factores clave que condicionan, de forma determinante, el futuro de las empresas y el comercio internacional.

Aunque la construcción naval se ha caracterizado, a lo largo de la historia, por ser un área claramente tradicional, en la que cualquier propuesta de evolución siempre ha encontrado múltiples detractores, le llegó el momento del cambio. Hoy en día, vemos drones sobrevolando los astilleros, modelos digitales virtuales de los buques antes de su construcción, pantallas táctiles, información digitalizada, así como la impresión de piezas complejas en impresoras 3D, actividades que hace unos cuantos años atrás parecían tomadas de la ciencia ficción.

Por lo general, algunos piensan que este cambio se aplica únicamente en la ingeniería, pero no es así. Hemos cambiado nuestra forma de reunirnos, nuestros lugares de trabajo, recibimos cientos de correos electrónicos y llamadas telefónicas en nuestros móviles, viajamos por todo el mundo sin billetes, entre otras acciones; por estos motivos, también han cambiado los negocios y las formas de llevar a cabo las contrataciones. Esto configura una voraz competencia que lucha por conseguir un mercado reducido en el que los actores se vean obligados a crear nuevas y atractivas iniciativas para los potenciales clientes.

La cooperación industrial es fundamental para la consecución de contratos de exportación, ya que la mayoría de países requieren que los acuerdos de defensa incluyan contenido local y/u otras contraprestaciones que retornen beneficios al país —puestos de trabajo, inversiones en nuevas capacidades, nuevas oportunidades de exportación o la reducción de la dependencia tecnológica de terceros—. La internacionalización, unida a los citados avances tecnológicos, facilita nuevos escenarios de contratación cooperativos en los que es posible compartir

conocimientos con el cliente, así como también las tecnologías de construcción y capacidades propias. Estas formas de contratación son las que podríamos definir como transferencia de tecnología (ToT).

Este sistema viene aplicándose desde hace algún tiempo y cobra fuerza con cada día que pasa. En la siguiente figura se indica la evolución que ha sufrido la demanda de transferencia tecnológica en el mercado internacional naval militar en los últimos años.

Figura 1: ToT como respuesta al mercado
Fuente: expuesto por el autor.

Es interesante analizar también cómo afecta la complejidad del producto requerido a la fórmula de contratación adoptada (ver figura 3).

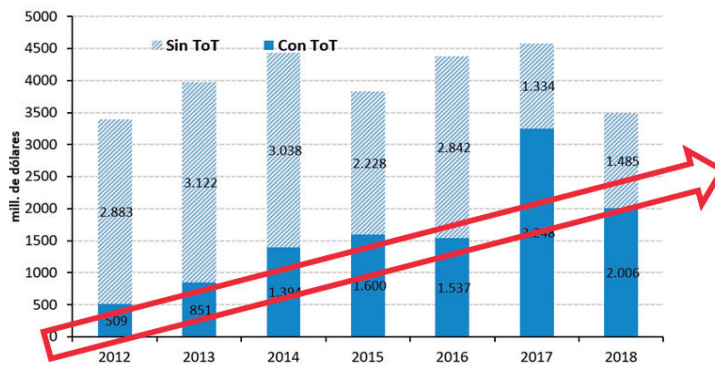


Figura 2: evolución de exportación naval militar de nuevas construcciones (2012-2018).
Fuente: SIPRI (Stockholm International Peace Research Institute).

Debemos tener en cuenta que este mecanismo de contratación, basado en la transferencia de tecnología, tiene muchas **ventajas** y algunos inconvenientes, tanto

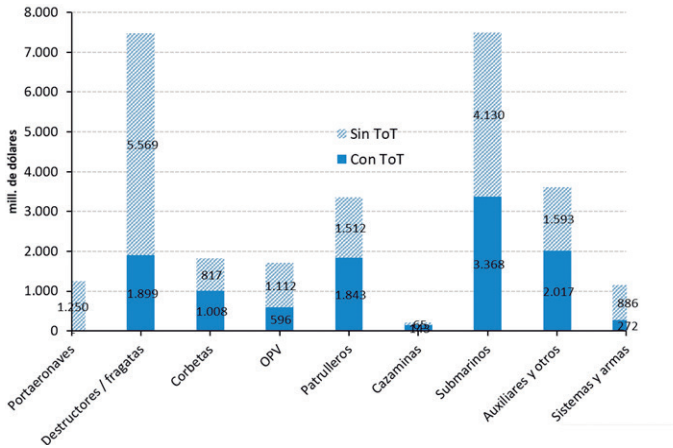


Figura 3: exportación naval militar por tipo de producto (2012-2018).
Fuente: SIPRI (Stockholm International Peace Research Institute).

para el emisor, como para el receptor. Una de las formas de elaboración de un convenio atractivo para ambos lados es el establecimiento del **equilibro**; por el lado del contratista, supone la mejora de su **competitividad**, en cuanto a la **rentabilidad** que le brinda el producto ofertado, hecho que le permite ingresar a un **mercado** aparentemente inaccesible. Asimismo, significa también el fomento de **nuevas relaciones** y la **fidelización** con el cliente, aunque cabe la posibilidad que en él exista una futura **competencia**. Por otra parte, aporta al cliente la transmisión en forma directa de **conocimiento** a **bajo costo**, permitiéndole el ingreso a un nuevo mercado y una contenida inversión con **riesgos mínimos**.

Figura 4: ventajas e inconvenientes en contratación ToT.
Fuente: expuesta por el autor.

Hoy en día, cada nuevo contrato requiere diferentes fórmulas que deben particularizarse tanto para el cliente como para el producto (ver figura 5). Algunas de las **soluciones** propuestas podrían necesitar el establecimiento local en el país, a través de la creación de una empresa, con el fin de proporcionar asistencias técnicas (in situ o mediante consultoría), negociar diferentes fórmulas de acuerdos de licencia, definir claramente los derechos de propiedad del producto, acordar la adquisición de determinados bienes o equipos, entre otras actividades.

Figura 5: ejemplos de mecanismos ToT.
Fuente: expuesto por el autor.

La combinación entre el **rol** requerido al contratista y el **alcance** solicitado puede dar lugar a múltiples combinaciones (ver figura 6). A ojos del cliente, esto es muy atractivo, ya que podrá variar desde el modelo tradicional de colaboración (diseño, aprovisionamiento y producción en instalaciones propias) hasta un modelo en el que se entrega el diseño, el aprovisionamiento y la producción de manos de un socio local, acordando entre ambos la adquisición de equipos, adiestramiento, y consultoría de ingeniería.

Respecto a ello, **Navantia** posee **vasta experiencia** en la formulación de contratos que impliquen transferencia

Figura 6: combinación rol/alcance requerido.
Fuente: expuesto por el autor.

de tecnología y cooperación para el desarrollo de la industria local, hecho que le ha permitido posicionarse estratégicamente como un **socio tecnológico de reconocido prestigio**. A continuación, les mostraré cómo se ubican los últimos contratos de Navantia, basados en diferentes **escenarios colaborativos ToT** con diversos países y productos, asumiendo diferentes roles y logrando distintos alcances.

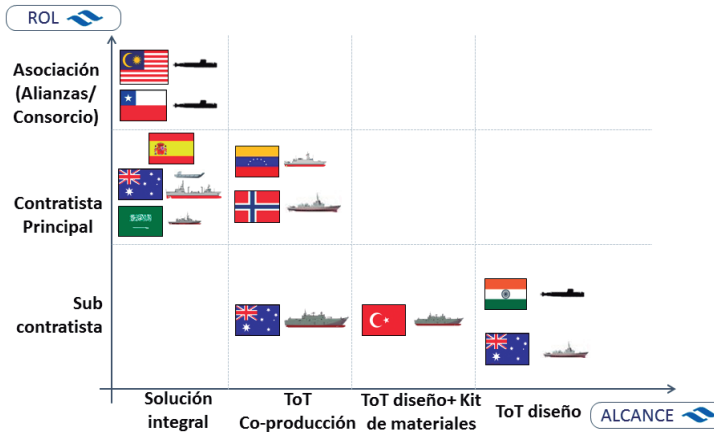


Figura 7: contrataciones ToT de Navantia
Fuente: expuesto por el autor.

Figura 8: buque Juan Carlos I (Armada Española).
Fuente: expuesto por el autor.

En tal sentido, sobresale el contrato para el ***Landing Helicopter Dock (LHD)*** firmado con Turquía, en el que Navantia, partiendo de un diseño probado (buque Juan Carlos I de la Armada Española) ha realizado el diseño de detalle del buque, considerando los requisitos de la Armada de Turquía y, además, suministra tanto los generadores diésel como el sistema integrado de control de plataforma (SICP).

Para el desarrollo de las actividades locales, Navantia estableció un *resident team* en Turquía, el cual colabora con las siguientes empresas:

- SEDEF. Contratista principal, socio local para la construcción en el astillero Tuzla de Estambul.
- Aselsan & Havelsan. Consorcio para el diseño y suministro del Sistema de Combate.
- Deltamarine. Empresa de ingeniería turca para el desarrollo de planos del diseño de detalle.
- AYESAS. Socio de Navantia para desarrollar el Sistema Integrado de Control de Plataforma (SICP).

Este contrato es un **claro ejemplo de éxito**, debido a que generó más de mil puestos de trabajo directos y siete mil indirectos en Turquía. Asimismo, representó el retorno del 100% de la inversión a compañías turcas, mediante un plan de participación industrial.

Asimismo, Navantia ha participado en otros grandes programas de cooperación industrial como el de los destructores AWD y buques anfibios ALHD para la Armada Australiana, los cuales fueron adaptados a los requisitos de sus clientes para generar el mejor producto.

Es preciso que concluya mi presentación asegurándoles que el **modelo de contratación basado en la transferencia de tecnología** vino para quedarse, ya que aporta **múltiples ventajas**, entre las que cabe destacar las siguientes:

- **Valor añadido** al producto
- **Reducción de riesgos**
- **Generación de empleos** y el consiguiente **impulso a la economía**
- Creación de **nuevas capacidades** para la industria naval
- Desarrollo de una **soberanía de capacidades industriales** en el ámbito naval, mediante la creación de un ecosistema de empresas autosuficiente y sostenible en el tiempo.

sesión

2.2

¿Cómo los aspectos de supervivencia impulsan el diseño de los buques de combate?

Ing.
Paolo Tornese

Al definir la supervivencia de un buque naval, la OTAN señala lo siguiente: “es la capacidad de seguir llevando a cabo sus misiones designadas en un entorno de combate”. De hecho, el elemento relativo a la capacidad de continuar la misión subyace en un aspecto clave de la supervivencia marítima. No basta con que el buque permanezca a flote, pues para sobrevivir debe esforzarse por continuar siendo eficaz en combate. El presente documento tiene por objeto proporcionar una visión general de los diferentes aspectos de la supervivencia de los buques navales, debatir las medidas y tecnologías actuales adoptadas para su mejora y destacar su impacto en el diseño de buques de combate. El programa FREMM italiano se presenta como un ejemplo exitoso de experiencia de diseño de embarcaciones de combate Fincantieri, con especial atención a las capacidades de supervivencia.

1. Introducción

En términos generales, la palabra supervivencia significa la capacidad de sobrevivir a una determinada situación. Sin embargo, en el contexto naval, la supervivencia tiene un significado específico y una aplicación mucho más amplia. Según la OTAN ANEP 43, contenido en el Manual de la OTAN sobre la supervivencia en combate de los buques (5) la supervivencia se define como: “la capacidad de un sistema de armas o un buque, para seguir llevando a cabo sus misiones designadas en un entorno de combate” (ver figura 1). Por lo tanto, no basta con que el buque permanezca a flote después de ser atacado, sino que la nave debe conservar cierto nivel de capacidades de combate para continuar su misión, aunque con un rendimiento degradado.

Según una definición análoga (10) la supervivencia se expresa mejor como producto de tres elementos principales: susceptibilidad, vulnerabilidad y la capacidad de ser recuperado. En este caso, la supervivencia de los buques se define de la siguiente manera: “la capacidad

de un buque y sus sistemas a bordo para evitar y resistir un entorno de efectos de armas sin sostener el deterioro de su capacidad, con el fin de llevar a cabo misiones designadas." La susceptibilidad se refiere a la incapacidad de una nave para evitar los sensores, armas y los efectos de estas en ese entorno hostil artificial. Al abordar la otra mitad de la frase clave, la incapacidad de la nave para soportar los efectos del entorno de combate se le denomina como vulnerabilidad (1). Según otras fuentes, la capacidad de recuperación puede incorporarse a la vulnerabilidad, concepto que se refiere a la facultad del buque y de la tripulación para contener daños y recuperar la capacidad degradada parcial o totalmente dentro de un plazo establecido y mantenerla durante un período determinado. La capacidad de recuperación, por otro lado, es una función del control de daños integrados a la nave, la asignación a bordo de equipos de control de daños y el entrenamiento y habilidades de la tripulación.

Como se muestra en la figura 1, una vez atacada la nave, los efectos de armas primarias, como los daños causados por explosiones, fragmentos, impactos y choques degradan

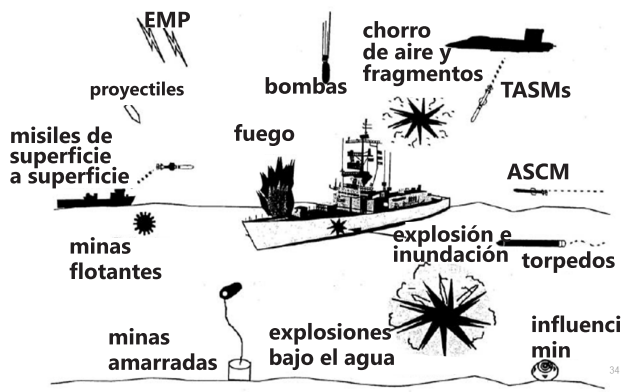


Figura I: armas y efectos contra amenazas de armamento. (10)
Fuente: expuest por el autor.

instantáneamente el nivel de operación, mientras que los efectos secundarios como el caso de los incendios, inundaciones, así como las fallas en el sistema y la estructura se degradan de forma lenta, pero significativa. Sólo los procedimientos de control de daños pueden restaurar parcialmente las capacidades de la nave (2); de hecho, la capacidad de recuperación abarca una gama más amplia de actividades que el control de daños (lucha contra incendios, control de inundaciones y reparación de emergencia) con el fin de mantener y recuperar las facultades. Después que el fuego se extinga, cuando las brechas queden selladas y el agua bombeada, la acción de recuperación continuará restaurando el estado operativo de la nave.

2. Definiciones

Al tratar de cuantificar la supervivencia global bajo los conceptos de susceptibilidad, vulnerabilidad y capacidad de recuperación, debe reconocerse que las palabras refieren complementos matemáticamente opuestos. La supervivencia es la capacidad para sobrevivir, así como la recuperación es la destreza para contener el daño y recuperar la facultad degradada y, por ello, necesitan maximizarse. La susceptibilidad y la vulnerabilidad representan la incapacidad para evitar o resistir los efectos del entorno hostil, por lo tanto, deben ser reducidas. Este punto no siempre se destaca claramente por las normas establecidas por las principales sociedades de clasificación (por ejemplo la OTAN ANEP-77, Código de Buques Navales). De hecho, el término genérico de la capacidad se utiliza indistintamente para abordar los diferentes aspectos de la supervivencia.

Por esta razón, la literatura científica sugiere que la supervivencia, la susceptibilidad, la vulnerabilidad y la capacidad de recuperación se definan como probabilidades (1), siendo P_s la probabilidad de que la nave sobreviva, P_n la probabilidad de que la nave sea alcanzada por un arma o sus mecanismos de daño, P_v la probabilidad condicional

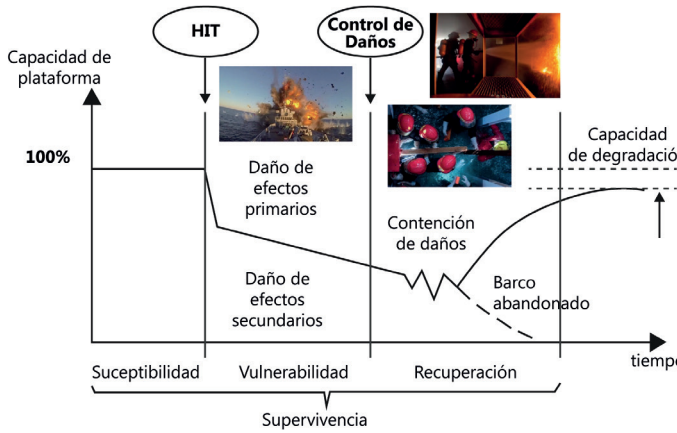


Figura 2: aspectos de la capacidad de Supervivencia.
Fuente: expuesto por el autor.

de que la nave fuese atacada dándole un golpe, mientras que P_R representa la probabilidad de que la nave se recupere después del golpe. Por tanto, se deduce que:

$$P_S = 1-[P_H \cdot P_V \cdot (1- P_R)] \qquad (1)$$

Algunos autores introducen el término *"killability,"* que es la probabilidad de que la nave sea asesinada, como complemento matemático de la supervivencia:

$$P_K = 1- P_S = P_H \cdot P_V \cdot (1- P_R) \qquad (2)$$

Al evaluar la susceptibilidad, se pueden considerar tres fases secuenciales: la probabilidad de que la amenaza esté activa, la probabilidad de detección, clasificación y objetivo de la nave por parte del enemigo, y la referida al arma del lanzamiento enemigo, vuelo e impacto:

$$P_S = 1-[(P_A \cdot P_{DCT} \cdot P_{LFI}) \cdot P_V \cdot (1- P_R)] \qquad (3)$$

La consideración del concepto de supervivencia tiene como fin mejorar este aspecto en una embarcación. Por otro lado, el reconocimiento de la relación entre los

diversos elementos combinados en el concepto general de supervivencia permite abordar la mejora de esta característica de forma coherente y completa.

3. Enfoque equilibrado de la supervivencia

La necesidad de integrar funciones mejoradas de supervivencia, para hacer frente a los efectos modernos de las armas de amenaza en el diseño de barcos, ha sido reconocida durante mucho tiempo. Por ejemplo, los daños potenciales causados por las armas modernas anti-buque quedaron demostradas por las diversas experiencias de ataques contra el HMS Sheffield, durante la Guerra de las Malvinas en 1982, y contra el USS Stark durante el Golfo Pérsico en 1987, hecho que también involucró el impacto de misiles Exocet en el USS Samuel B. Roberts (1988), USS Trípoli y USS Princeton (1991), que a su vez implicaron incidentes de minería de contacto y ráfaga de proximidad.

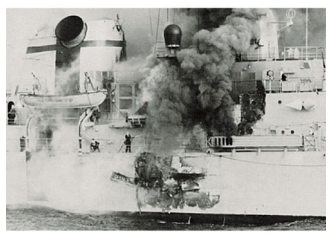


Figura 3: el HMS Sheffield en llamas después de ser impactado por un Exocet, (12)
Fuente: UK Mod.

Figura 4: el USS Stark luego de ser atacado por dos misiles Exocet Iraquíes en el Golfo Pérsico.
Fuente: USN – dominio público.

Figura 5: el casco dañado del USS Samuel B. Roberts,(12).
Fuente: PH2 Rudy D. Pahoyo.

Figura 6: USS Trípoli después de ser atacado por una mina Iraquí.
Fuente: JOI Gawlowicz – USN.

En ese sentido, un buque naval debe poseer muchos atributos para cumplir con sus requisitos impuestos y, por tal motivo, la mayoría de estos entran en conflicto; por lo tanto, las compensaciones son necesarias durante el proceso del diseño y la supervivencia se convierte en un atributo importante que debe ser tomado en cuenta (1). Precisamente, esta característica se maximiza al producir diseños en los que la susceptibilidad, vulnerabilidad y la capacidad de recuperación estén equilibrados (9).

Durante los años 60 y 70, se estableció que las armas nucleares representaban una amenaza tan abrumadora para los barcos que había poca necesidad de enfatizar características que les permitieran sobrevivir a los daños. De ahí proviene la máxima que señala que un barco atropellado es un barco perdido. Por lo tanto, se puso especial énfasis en las capacidades ofensivas, así como en las facultades de sigilo y las medidas de engaño o destrucción de amenazas.

Sin embargo, las reglas de combate se incrementaron junto con las operaciones en el agua del litoral y la proliferación de armamento sofisticado. Por otro lado, también se dieron cambios en la situación mundial y la creciente probabilidad de que los buques se encuentren involucrados en combate, aún en tiempos de paz, periodo en el que todos trabajan para evidenciar que la otra mitad de la supervivencia necesita considerar aspectos como la capacidad de sobrevivir a un golpe (1). Por lo tanto, se considera que el equilibrio de las características de la embarcación entre los tres componentes de supervivencia es de vital importancia (8). Durante la Guerra de las Malvinas, por ejemplo, 16 buques fueron alcanzados mientras participaban en operaciones de combate, de un total de 23 fragatas o destructores; es necesario recordar también que un beneficio adicional a la mayoría de características de reducción de la vulnerabilidad es que mitigan los efectos de incendios, colisiones, puestas a tierra u otras bajas no causadas por arma de fuego.

Figura 7: el USS Cole es remolcado lejos de la ciudad portuaria de Adén, Yemén después del bombardeo.
Fuente: Sargento Don L. Maes – USN – Dominio público.

Después de todo, es poco práctico diseñar una embarcación invulnerable. Respecto a esto, podemos mencionar una consideración interesante (9). Se comparan los dos extremos referidos a la susceptibilidad cero y la vulnerabilidad cero. Una embarcación con capacidades de defensa absolutamente infalibles sería totalmente superviviente contra amenazas hostiles hechas por el hombre porque, incluso si fuera altamente vulnerable, ningún arma de podría golpearla. Sin embargo, un buque con cero susceptibilidades y con poca inversión en reducción de vulnerabilidad, sólo sobreviviría plenamente al emplear sus defensas. Asimismo, permanecería vulnerable aunque sus defensas estuviesen activas (por ejemplo, si permaneciese anclado en un estado de no-alerta en un puerto extranjero, como en el ataque terrorista contra el US Cole en el 2000, mientras el destructor estaba en puerto y era reabastecido en el puerto Yemení de Adén, como se aprecia en la figura 7). Si fuese muy vulnerable, podría quedar fuera de acción.

En el otro extremo, una embarcación totalmente invulnerable sería completamente superviviente pues, aun siendo golpeada varias veces, no sería eliminada. Desafortunadamente, una nave cuya principal fortaleza fuese la capacidad de absorber daño sería demasiado pesada, costosa e inmóvil para ser un combatiente efectivo. Es evidente que ningún extremo desarrollaría una embarcación efectiva.

La imagen incisiva de un péndulo se utiliza para explicar el énfasis en la reducción de la vulnerabilidad. Por lo general, oscila en la dirección de la reducción de la debilidad

después de sufrir daños en tiempos de guerra o accidentes en tiempos de paz y se aleja a medida que avanza el tiempo y los recuerdos se desvanecen. La reducción de la vulnerabilidad es generalmente conocida como la "hermana pobre" entre las capacidades que normalmente se comercializan en el proceso de diseño de buques. Esto se da principalmente en buques pequeños, en los que no se pueden acomodar fácilmente el blindaje y otros sistemas de protección. Además, bajo las presiones de recorte de costos, las características de reducción de vulnerabilidad pueden recibir baja prioridad al ser menos visibles y podrían carecer de apoyo por parte de la autoridad superior.

Aunque algunos requisitos de reducción de la vulnerabilidad, como la estabilidad de daños y la longitud inundable, son considerados como sacrosantos y no están sujetos a compensación, otras características han tomado un lugar secundario para el diseño de buques como el peso, la velocidad, los sistemas de armas y el costo. Sin embargo, muchos aspectos de la reducción de vulnerabilidades pueden ser incluidas en dicha labor sin que esto suponga un aumento significativo de costos o impactos adversos en el diseño, siempre y cuando se identifiquen a tiempo. Desafortunadamente, tales características todavía tienden a ser percibidas como complementos que tienen poco propósito útil en apoyo de las misiones primarias de la embarcación.

3.1. Características de Susceptibilidad

La premisa básica en cuanto a la reducción de la susceptibilidad radica en que es mejor evitar un golpe que soportar uno. Es mejor esconderse que dañar, mejor destruir una amenaza a distancia que resistir el daño de un golpe exitoso.

Como se explicó anteriormente, cualquier medida adoptada para reducir la probabilidad de ser atacado está dentro del régimen de susceptibilidad. En tanto, es posible identificar los siguientes cuatro pasos necesarios (8):

- Evite ser detectado.
- Si se detecta, evite ser identificado.
- Si se identifica, evite ser objetivo.
- Si es objetivo, evite ser atacado.

Lo anterior puede lograrse mediante una mayor conciencia situacional, la gestión de la marca de la embarcación (elemento pasivo) y la capacidad de una fuerte autodefensa, incluida las capacidades de eliminación dura y suave (elemento activo).

Cabe señalar que debe lograrse un equilibrio entre la reducción de marcas y la capacidad de autodefensa, siendo el principal objetivo de la primera generar mayor eficacia en el funcionamiento de las medidas de eliminación blanda.

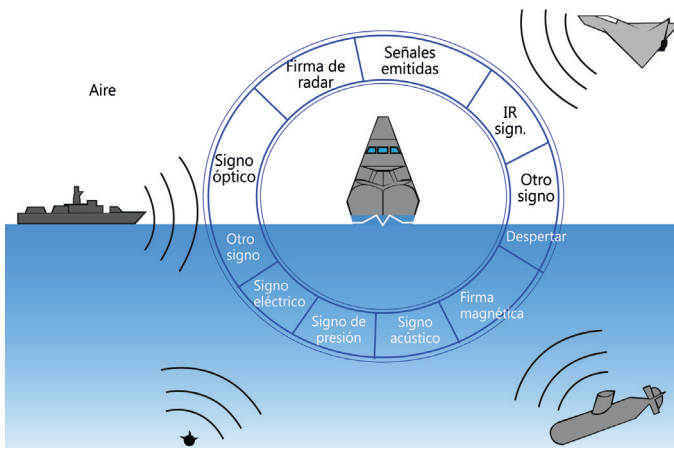


Figura 8: marca de Embarcaciones (7).
Fuente: expuesto por el autor.

Un nivel bajo de la marca puede hacer que la amenaza no participe correctamente (ver figura 8). De hecho, el objetivo general es reducir la capacidad de detección a un nivel aceptable, en lugar de hacer que la nave sea invisible. Además, la gestión de marcas es importante, ya que es

incluida en la ubicación de los golpes de muchos tipos de armas, dependiendo de su sistema guía.

La marca se divide en diferentes categorías, por encima y por debajo de la superficie marina. Asimismo, las marcas de los buques sobre el agua incluyen la óptica, el radar y la emisión de rayos infrarrojos, mientras que las marcas subacuáticas están compuestas por las variables de electricidad, presión, acústica, magnética y secuelas.

Por otro lado, la evolución de las tecnologías permite una reducción significativa en todos los tipos de marcas, pero no siempre son operativamente eficaces o rentables. En tanto, las tácticas también pueden ser un elemento significativo en la gestión de las marcas.

Además de las marcas y el conocimiento de la situación, el componente esencial restante de la susceptibilidad es la capacidad de autodefensa de la embarcación. El objetivo es destruir, degradar o engañar a la amenaza dirigida hacia la embarcación. Tradicionalmente, la nave se basa en sistemas de defensa, incluidos los componentes de muerte dura y suave. Los sistemas de eliminación dura tienen como objetivo destruir las armas entrantes en vuelo, por ejemplo, si en caso una nave de largo y mediano alcance lanzase misiles defensivos para defensa exterior o los sistemas de armas de cierre CIWS para la defensa interna. A las acciones de muerte blanda también se les conoce como Contramedidas Electrónicas (ECM) y son definidas como técnicas y equipos que contrarrestan el uso de la electrónica por parte del enemigo. Las ECM incluyen las interferencias de radares, IR y comunicaciones, falsos objetivos electrónicos, dispositivos de bloqueo de misiles y señuelos tales como “chaff”, “basura” y bengalas IR, que se pueden utilizar para generar distracción al presentar objetivos alternativos ante un radar de misiles durante su fase de búsqueda (1).

3.2. Características de vulnerabilidad

Al igual que con la susceptibilidad, las medidas de reducción de vulnerabilidades configuran un proceso de varias etapas, las cuales mencionaré a continuación (8):

- Si se ataca, evite ser dañado.
- Si está dañado, continúe luchando.
- Si no pueden seguir luchando, permita que la capacidad se retire.
- Si está lisiado, deje tiempo para evacuar.

Las medidas que contribuyen al logro de estos objetivos incluyen un diseño estructural eficiente, una subdivisión indiscutible y una buena estabilidad de daños, divisiones de incendios y la minimización del uso de material inflamable, zonificación y contención para limitar los daños causados por ataques nucleares, químicos y biológicos (14), localizar componentes vitales en lugares protegidos, proporcionar redundancia (mientras separa elementos redundantes) y componentes de protección (1).

3.3. Características de recuperación

Los siete pilares claves de la capacidad de recuperación, definidos por el Ministerio de Defensa del Reino Unido, junto con sus componentes claves pertinentes son los siguientes (ver figura 9):

- Concientización sobre la situación.
- Administración.
- Contención.
- Procesamiento.
- Recuperación.
- Asistencia externa.
- Escape y evacuación.

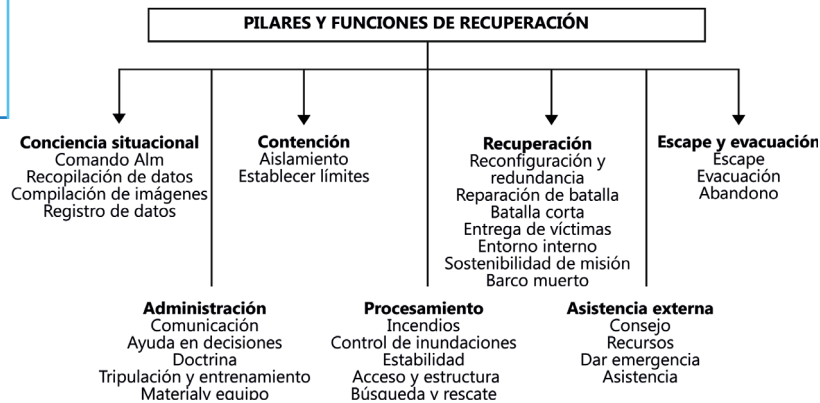


Figura 9: pilares de Recuperación. (8).
Fuente: expuesto por el autor.

Un aspecto importante de la capacidad de recuperación es mantener una organización eficiente y eficaz. Esto se hace posible al asignar los niveles adecuados de dotación y habilidad a los diferentes rangos, definir las condiciones de preparación, mantener e inspeccionar regularmente el equipo y la capacitación, los medios de detección, evaluación y acción contra daños que serán rápidos y eficaces.

Experiencias pasadas en tiempos de guerra nos han enseñado muchas lecciones sobre la importancia de la capacidad de recuperación y el control de daños. Es bien reconocido que el USS Stark se salvó gracias a las acciones de control de daños y los esfuerzos heroicos de la tripulación. Una historia similar se puede contar del USS Samuel B. Roberts.

4. La experiencia italiana FREMM

La experiencia italiana del programa FREMM, de Multi-Misión Europea de Fragata, es un proyecto conjunto de cooperación industrial de defensa ítalo-francesa que representa el resultado de un requisito que surgió a finales de la década de 1990, para que Italia y Francia renueven la

mayor parte de sus escoltas de superficie de primera línea frente a la obsolescencia de bloques de las embarcaciones existentes (13). La estructura industrial del nuevo proyecto se basa en la utilizada para los destructores de defensa aérea Horizon. En el caso de Italia, la entrega del programa fue confiada al consorcio ***Orizzonte Sistemi Navali*** (OSN) de Fincantieri y Finmeccanica, ahora conocida como Leonardo, trabajando en colaboración con la empresa conjunta francesa similar ARMARIS, entre DCN (ahora Grupo Naval) y THALES. Una atracción clave del concepto FREMM para ambas marinas es la capacidad de configurar un diseño común de diferentes roles, a través de cambios limitados en el equipo. En el caso de Italia, su requisito es obtener sub-clases separadas de uso general (GP) y anti-submarinas (ASW). Las fragatas de la Armada Italiana se construyen en el astillero naval integrado de Fincantiere, el cual utiliza instalaciones complementarias divididas entre Riva Trigoso, cerca de Génova, y Muggiano, junto a La Spezia, en el mar de Liguria. Los dos primeros FREM italianos, que fueron el***Carlo Bergamini***, en su versión GP, y ***Virginio Fasán***, en la versión ASW, fueron entregados durante el 2013 y se espera que el total de entregas concluya en el 2021. En febrero del 2018, la US Navy adjudicó un contrato de diseño conceptual de $15 millones a la filial de Fincantieri, Marinette Marine, para transformar el diseño FREMM en fragatas de nueva generación para su programa FFG. Por otro lado, Australia pre-seleccionó fragatas FREMM paras su proyecto de fragatas Mar 5000 Future, para septiembre del 2017.

4.1. Capacidades de supervivencia de FREMM

Los FREMM italianos tienen un desplazamiento de carga completa de aproximadamente 6,500 t., una longitud total de unos 144 m. y una velocidad máxima superior a los 27 kn. La resistencia de los buques es de hasta 45 días continuos, mientras que su alcance es de 6,000 NM a 15 Kn. Asimismo, pueden desempeñar el papel del grupo de tareas del comandante. Los buques están diseñados

y construidos en base al RINAMIL para las reglas del FREMM. Por otro lado, la planta de propulsión tiene una configuración CODLAG (eléctrica y combinada con gas diésel) con una turbina de gas, dos motores eléctricos de tipo reversible, hélices de paso controlable y cuatro grupos electrógenos diésel. Ambas versiones (GP y ASW) están equipadas con una sonda montada en la proa. La versión ASW también está equipada con un sonar de profundidad variable (VDS) y embarca dos cañones STRALES de 76/62 mm. Ambas versiones están equipadas con 2 RHIB grandes y la versión GP puede operar con un barco de las fuerzas especiales de 11,3 m., situado a popa; además, la versión GP prevé un cañón Vulcano de 127/64 mm., en lugar de una de 76 mm. Ambas versiones tienen dos hangares para dos helicópteros, ya sea dos SH90 o uno SH90 + un EH101.

Ambas sub-clases italianas FREMM están equipadas con una amplia gama de contramedidas para complementar sus sistemas de armas. El conjunto de guerra electrónica, que incluye las medidas de apoyo electrónicas por radar (ESM) y el ESM de Comunicaciones, así como los jammer (conocidos también como perturbadores), se complementa con las contramedidas físicas, en particular los dos señuelos lanzadores OTO MELARA SCLAR-H y, limitado a la configuración antisubmarina, un sistema de defensa de torpedos SLAT.

El estrecho nivel de atención prestado a las diversas contramedidas de la clase se iguala por el énfasis en las capacidades de sigilo. Además de abarcar medidas para reducir la sección transversal del radar de las fragatas, lo cual es evidente en el diseño del casco y la superestructura, incluye también la reducción de la firma infrarroja y acústica. Esta última es particularmente importante para la configuración ASW, donde el elemento eléctrico del sistema de propulsión CODLAG permite un funcionamiento silencioso hasta con velocidades de alrededor de 15

nudos, desconectando la caja de engranajes. Esto se ve mejorado aún más por la especificación de hélices de paso controlable, que pueden ser menos fáciles de detectar y analizar por parte de los submarinos. Además, son capaces de ofrecer una mayor maniobrabilidad.

Garantizar la supervivencia en caso de daño ha sido otra consideración clave del diseño. Por ejemplo, áreas claves como el CIC y el tronco de comunicaciones verticales están protegidas contra armas pequeñas y daños de metralla por estructuras blindadas, mientras que las consolas están montadas en impactos.

Los cascos de las fragatas se dividen en once compartimentos principales y permanecerán estables con al menos tres de ellos inundados. A su vez, hay dos zonas principales y autónomas de control de daños, las cuales son capaces de operar en forma totalmente independiente con respecto a la generación y distribución de energía eléctrica. Cada una está equipada con un centro de control de daños para la gestión de la defensa pasiva.

También hay un propulsor retráctil de ACIMUT eléctrico de 1MW situado en la parte delantera de la sala de máquinas auxiliares, el cual soporta una capacidad de hasta siete nudos de velocidad en condiciones de ser llevado a casa. Toda la necesidad eléctrica requerida por el buque y el TAR podría ser alimentado por dos de los cuatro DE y la DG, situados cerca del propio ART, siguiendo los principios de concentración para la reducción de la vulnerabilidad.

5. Conclusiones

Hasta aquí, hemos presentado la supervivencia de los buques combatientes y sus aspectos relacionados, proporcionando ejemplos de medidas y tecnologías para su mejora y destacando su impacto en el diseño general de la nave.

Como bien sabemos, el diseño de buques es un proceso iterativo, a menudo representado en forma de espiral

de diseño y que implica una multitud de variables, especialmente en el área del diseño de buques de guerra altamente complejos con los que el arquitecto naval tiene que llegar a una solución equilibrada. Durante las primeras etapas de diseño, las concepciones de los buques son susceptibles a ser modificadas, lo que sería caro o incluso inviable en las etapas posteriores. Por lo tanto, es importante que la supervivencia se cuantifique y sea considerada durante estas etapas, para ofrecer mayor certidumbre y confianza para el diseñador y para el cliente, en el sentido de que se cumplirá su requisito. Además, la cuantificación de la supervivencia justificaría las características de mejora de la misma, desalentando la reducción de costos en esta área.

Queda establecido, además, que los tres componentes de la supervivencia referidos a la susceptibilidad, la vulnerabilidad y la capacidad de recuperación deben ser considerados y evaluados por igual, para que se intente obtener un equilibrio entre las características de supervivencia (8). Como se ha señalado, es extremadamente poco práctico diseñar un barco invulnerable. Por otra parte, no se ha demostrado que ningún extremo pueda crear un barco eficaz.

Por último, la experiencia de diseño italiana FREMM se ha presentado como un ejemplo exitoso de nave de combate moderna y capaz de alcanzar altos estándares de supervivencia.

Referencias

A. Ungaro & P. Gualeni (2015), *Un Resumen de data de daños de los Buques de Guerra desde 1967 hasta el 2013. Procedimientos sobre la 12° Conferencia Internacional sobre Estabilidad de Embarcaciones y Vehículos del Océano*, Stab2015. Reino Unido: Glasgow.

A.S. Piperakis (2013), *Un enfoque integrado para la supervivencia de buques navales en el diseño preliminar de buques*. Tesis doctoral UCL. University College London.

C. Aguas, FREMMS Italiano (2014). En C. Waters, Seaforth, *Revisión Naval Mundial 2015*. Publicación Seaforth. Reino Unido, Barnsley.

D.G.M. Watson (1998), *Diseño Práctico de Buques*. En Elsevier Science ltd. Reino Unido: Oxford.

DNV GL. (2007), Reglas para la Clasificación: Buques Navales.

E. Boulougoris & A. Papanikolaou (2013), *Diseño basado en Riesgos de Combatientes Navales. Ocean Engineering* 65 , 49-61.

Equipo de especialistas del Grupo Naval 6 de la NATO sobre diseño de buques pequeños (2004), *Documento de trabajo de la NATO/PfP sobre el diseño de buques pequeños, documento no-clasificado NATO/PfP.*

Lloyd's Register (2019), Reglas y Reglamentos para la Clasificación de Buques Navales.

M.O. Said (1995), Teoría y Práctica de la Supervivencia Total de Buques para el diseño de Buques. Naval Engineers Journal 107 (4), 191-203.

NATO, "Publicación de Ingeniería Naval Aliada sobre Supervivencia en Combate de Buques" (ANEP-43). Edición 2, Documento clasificado de la NATO, 2003.

NATO (2019), Publicación de Ingeniería Aliada Naval, Código de Embarcación. ANEP-77 (ed G.) (versión 2).

R. Bell & C.N. Calvano (1994), Estableciendo los Fundamentos de una Disciplina de Diseño de Supervivencia de Buques de Superficie. Naval Engineers Journal 106 (1), 71-74.

R.M. Reese, C.N. Calvano & T.M. Hopkins (1998), Requisitos de Vulnerabilidad orientados operacionalmente en el Proceso de Diseño de Buques. *Naval Engineers Journal* 110 (1) , 19-34.

S.D. Turner, P. Horstmann & G. Brain (2006), *Supervivencia de los Buques de Guerra, Procedimientos RINA de Buques de Guerra 2006: Barcos de Superficie del Futuro*. Reino Unido: Londres.

BLOQUE 3

SISTEMA DE ADMINISTRACIÓN DE COMBATE

BLOQUE

3

MODERADORES

EXPOSITORES

SESIÓN 3.1

Calm.
Jorge
Andaluz Echevarría

Quiero agradecer la presencia del Vicealmirante Manuel Antonio Martínez Ruiz, director de Ingeniería y Construcción Navales de la Armada Española y al Ingeniero David Mancera, representante de Navantia System.

El tema que nos aboca esta mañana guarda relación con los sistemas de administración de combate o CMS, los cuales se constituyen actualmente como el cerebro y pieza fundamental de todas las plataformas navales que se construyen. Actualmente, los gestores, ingenieros, aquellos que configuran las plataformas de superficie y, sobre todo, los que se dedican a visualizar el trabajo de un sistema de administración de combate tienen un enorme reto, el cual se define fundamentalmente por el tiempo en que una plataforma es concebida y en que un buque es comisionado.

Este proceso, aunque parezca increíble, puede tomar entre diez y veinte años en ser implementado. Tal es el caso de la Armada Española que, en estos momentos, no solo están pensando en las fragatas F110, sino también en las futuras F120, habiéndose comisionado hace poco la nave Cristóbal Colón, último buque de la clase F100. El tiempo establecido nos obliga a visualizar las futuras amenazas; en el caso de la Marina de Guerra del Perú, al comisionar cualquier buque, se hace junto con un misil anti buque determinado y es muy probable que este pase a la reserva con otro sistema de armas. Esto nos lleva a pensar en que las armas anti buque tienen, en cuestiones de tiempo, un desarrollo mucho menor que el ciclo de vida de la plataforma. Por eso los

CMS deben tener escalabilidad, es decir, cierto porcentaje y reserva de crecimiento, para ser compatibles con las futuras amenazas y misiones que se presenten.

Asimismo, tienen que ser adaptables para enfrentar las diferentes misiones. Particularmente, la Marina de Guerra del Perú afronta un reto muy importante desde el año 2004, periodo en el que comenzamos a desarrollar nuestro propio sistema de combate, el cual ha alcanzado un aceptable nivel de maduración.

En el caso de la Armada española, supuso un verdadero reto desarrollar un sistema de combate y mantener una gradualidad en el tiempo, sobre todo para lograr la integración de los sistemas más modernos y potentes construidos hasta hoy. Este es el caso del radar SPI-1, el cual dota a los buques clase F110 de toda clase de informaciones, lo que obliga a tener sistemas de gestión y administración de combate muy desarrollados, con una velocidad de procesamiento de toda la información proporcionada.

En ese sentido, la experiencia de éxito que tuvo la Armada española con el SCOMBA, con el sistema de combate de la Armada, así como la escalabilidad y adaptabilidad de los sistemas serán tocados en este foro. Sin más preámbulo dejo con ustedes al Ingeniero David Mancera de Navantia System.

sesión

3.1

Asegurando un alto nivel de adaptabilidad y escalabilidad en los sistemas de combate modernos

Ing.
David
Mancera Araujo

Los sistemas de administración de combate, presentes en la práctica total de los buques de guerra actuales, están dotados de una gran complejidad y requieren de grandes inversiones para su diseño y desarrollo (tanto en tiempo como de otros recursos). El aseguramiento de su capacidad de adaptación, en base a nuevos requisitos y misiones, se ha convertido en una necesidad fundamental para garantizar el uso óptimo de esos esfuerzos. El presente documento describirá tres de los parámetros no funcionales que ejercen mayor incidencia en la capacidad de adaptación futura y la maximización de la vida útil de un CMS, analizando la forma en que el correcto dimensionamiento de dichos factores influye en la arquitectura del sistema y propone un conjunto de recomendaciones para su optimización y vigilancia.

1, Introducción

Los sistemas de administración de combate naval hacen un uso masivo de aplicaciones y software, para desempeñar misiones en escenarios complejos con la adecuada flexibilidad, proporcionando a la tripulación del buque capacidades óptimas de conciencia situacional, así como también de inteligencia, ayuda a la decisión y control de los actuadores para la correcta ejecución, monitorización, evaluación de los enfrentamientos, la garantía de la defensa del buque y las unidades bajo su protección.

Los sistemas de administración de combate (Combat Management System en inglés) forman parte de sistemas mayores en los que la interoperabilidad con buques de la misma Marina de Guerra, o de otras instituciones, se convierte en un elemento esencial de la misión. Asimismo, el uso del CMS se da a lo largo de toda la vida útil del buque, la cual se prolonga por lo general en decenas de años.

Por si fuera poco, a este escenario de enorme complejidad se le suma el hecho que la industria de la defensa a nivel mundial está experimentando un momento de profunda

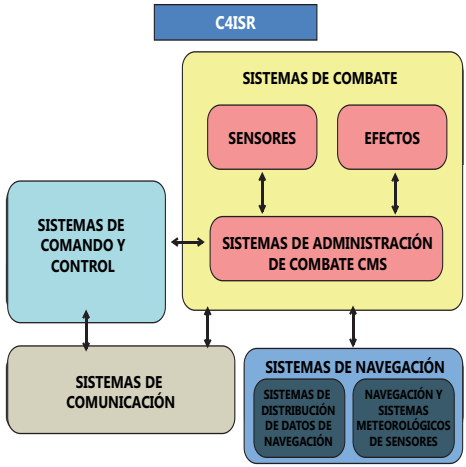


Figura I: sistemas de administración de combate en el contexto de los sistemas C4ISR.
Fuente: expuesto por el autor.

transformación y que, aun afectando a todos sus niveles y componentes, quizás encuentre un énfasis especial en los denominados sistemas de mando y control, categoría en la que se circunscriben los CMS. Por un lado, esto se debe fundamentalmente al aumento progresivo de la necesidad de adoptar medidas de ciberseguridad que garanticen la inviolabilidad de los sistemas, en un medio cada vez más complejo y abierto. Esto se evidencia en el uso creciente de comunicaciones inalámbricas y servicios alojados en la nube; por otra parte, encontramos el fenómeno de la creciente aplicación en defensa de las tecnologías de inteligencia artificial, especialmente las relacionadas con el denominado *machine learning*, que empezó a utilizarse de manera transversal en los últimos años en la totalidad de dominios y funciones de los sistemas de mando y control, incorporando nuevas capacidades de autoaprendizaje y mejoras significativas en la asistencia a los usuarios.

Por tanto, es necesario que los CMS dispongan de una arquitectura que garantice su adaptabilidad y escalabilidad en este escenario que *abraza el cambio* y evoluciona a un ritmo vertiginoso y distinto al de décadas anteriores. La naturaleza informática de los sistemas de administración de combate aconseja que cualquier estrategia que persiga este objetivo (referido a la extensión de la vida útil, aumentando la capacidad de adaptación a los requisitos

emergentes) necesita apoyarse en una revisión profunda de los factores que determinan la idoneidad de dicha arquitectura. En este caso, los denominados parámetros no funcionales o parámetros de calidad ejercen un papel indiscutible.

En este estudio, centraremos nuestra atención en tres de esos parámetros para responder a la siguiente pregunta: ¿cómo construir sistemas de administración de combate adaptables y escalables? De este modo, veremos que la capacidad de adaptación implica sistemas que puedan adecuar su comportamiento a la totalidad de sus usuarios, bien de forma autónoma (adaptatividad), bien de manera asistida por el propio usuario (adaptabilidad), pero siempre a partir de información adquirida acerca de los propios usuarios y su entorno; por otro lado, la escalabilidad hace referencia a la capacidad del sistema de extender su comportamiento, permitiendo la ejecución de nuevas funciones y facilitando su crecimiento futuro más allá de la línea base entregada tras la liberación inicial del sistema, ya sea mediante la adición de una nueva funcionalidad o a través de la modificación de la existente.

Ahora bien, ¿cómo abordar este problema? ¿Cómo asegurar que un sistema de administración de combate dispondrá de las propiedades que le permitirán adaptarse a sus usuarios, al entorno de ejecución, a las diferentes misiones de los buques en los que se instale y los nuevos requisitos? Finalmente, ¿cómo garantizar que el sistema ofrece facilidades para su mantenimiento?

En esta presentación discutiremos estas cuestiones, describiremos las características de una arquitectura que permita cumplir este objetivo y propondremos un conjunto de recomendaciones para alcanzarlo, sin perder de vista la importancia de los equipos humanos que realizan los trabajos de diseño, implementación y mantenimiento de los sistemas.

2. Requisitos significativos para la arquitectura de un sistema software

Cualquier sistema basado en el uso de computadoras necesita optimizar un número significativo de requisitos, llamados también atributos de calidad, a partir de los cuales se medirá y calificará el rendimiento del sistema. Los sistemas de administración de combate, al igual que los sistemas computarizados, no son la excepción a esta regla. Entre los atributos de calidad más conocidos, particularmente en los sistemas en los que la seguridad es un factor crítico, podemos destacar los factores de fiabilidad, disponibilidad, mantenibilidad y seguridad, que comúnmente aparecen agrupados por las iniciales de sus nombres en inglés, bajo el acrónimo RAMS *(reliability, availability, maintainability, safety)*.

Sin embargo, al referirnos a sistemas software, no todos los requisitos no funcionales afectan a la arquitectura del sistema, así como tampoco solo los de ese tipo lo hacen. En cuanto a los atributos relacionados con la arquitectura del sistema, suelen agruparse bajo la denominación *architecturally significant requirement (ASRs)*; en líneas generales, los ASR definen características fundamentales del sistema software, imponen restricciones y caracterizan el entorno en el que se desenvolverá el sistema. Su importancia es clave, puesto que la mayor parte de las decisiones tomadas durante la etapa de diseño, en relación a la arquitectura, girarán alrededor de alguno de ellos. Esto significa que, en última instancia, el sistema de administración de combate debe cumplir con los objetivos que resumíamos en la introducción y su diseño tiene que garantizar la adaptabilidad y escalabilidad futuras, lo cual dependerá del valor que los arquitectos software otorguen a los ASR.

En ese sentido, existen más de cien requisitos significativos para la arquitectura. No pretendemos cubrirlos todos, pero sí incidir en aquellos que, a nuestro juicio, tienen mayor

impacto en la capacidad de evolución futura de los CMS, como es el caso de la adaptabilidad, escalabilidad y mantenibilidad.

2.1. Adaptabilidad

Debido a su amplitud, la palabra adaptación define de manera más adecuada el concepto que se pretende explicar. En el caso de las Ciencias de la Computación, la adaptación se refiere al proceso mediante el cual un sistema interactivo adapta su **comportamiento al de sus usuarios, a partir de la información** adquirida sobre este y su entorno. Asimismo, el cambio puede darse de dos maneras:

- Cuando el sistema ofrece herramientas para que el propio usuario lo personalice de manera sustancial, nos referimos a la adaptabilidad propiamente dicha.
- En caso el sistema sea capaz de adaptarse al usuario de manera automática, de acuerdo con las condiciones cambiantes, estaríamos hablando de la adaptatividad, término que aún no ha sido recogido por los diccionarios y que proviene del inglés *adaptivity*. Por eso, algunas personas se refieren a estos sistemas como adaptativos.

Ambas acepciones se aplican en los sistemas informáticos en general y en los de administración de combate en particular. Asimismo, son complementarios entre sí y contribuyen a incrementar la correspondencia entre las necesidades del usuario y el comportamiento del sistema una vez finalizado su desarrollo y tras la entrega al usuario final.

A continuación, revisaremos los principales casos y ejemplos de cada uno de estos.

- **Adaptación al usuario**

  Aunque un buen proceso de diseño centrado en el usuario garantiza cierto grado de aceptación, la

capacidad de un sistema para adaptarse a condiciones cambiantes juega un papel muy importante en el objetivo de lograr dicha aceptación. Los diseñadores del sistema deben asumir que es difícil anticipar las posibles modificaciones de requisitos y, por la dinámica intrínseca de las condiciones de uso cambiantes, conviene desplazar el proceso de personalización de las características del sistema desde la fase de desarrollo hacia la de operación, hecho que implicará la implementación de técnicas de adaptación en el sistema para reaccionar a dichas condiciones cambiantes lo más rápido posible. Esto permitirá que el sistema sea adaptable o adaptativo, o bien, en el mejor de los casos, ambas cosas.

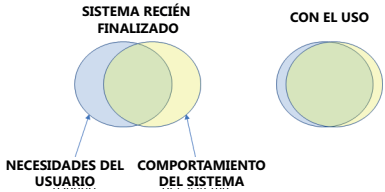


Figura 2: objetivo de adaptabilidad de un sistema de administración de combate.
Fuente: expuesto por el autor.

En términos generales, la adaptación al usuario recae bajo una de las dos premisas siguientes:

- *Adaptación a los diferentes usuarios*

  Los usuarios finales serán heterogéneos y el sistema debe ser capaz de anticiparse a esta circunstancia y ofrecer los mecanismos adecuados para todos ellos.

- *Adaptación a un mismo usuario a lo largo del tiempo*

  Esto se refiere a que las competencias y expectativas de los usuarios finales también evolucionarán a lo largo del tiempo. El sistema debe ofrecer diversas opciones, tanto al operador novato como al experto, con el objetivo de facilitar el aprendizaje del primero y evitar la frustración del segundo.

- **Adaptación al entorno**

  Aunque sabemos que un sistema software se adapta a los usuarios a partir de la información obtenida de los

mismos y del propio entorno, lo cierto es que el sistema debe adaptarse al entorno, el cual puede ser igualmente heterogéneo y/o dinámico. Las tres situaciones más frecuentes son:

- *Adaptación al entorno de ejecución*

  El sistema tendrá, por lo general, un entorno de uso habitual (Centro de Operación y Control) y otros de uso minoritario, desde donde accederá a sus capacidades en la totalidad, en parte o en función del tipo de buque (puente, locales de equipos, etc.) ya sea mediante la detección automática de las diferencias entre entornos y la respuesta automática que permitirá la adaptación al mismo; en lo referido a la capacidad de configuración de manera adaptada durante la instalación, a través de herramientas proporcionadas a los usuarios para que sean ellos los que particularicen el sistema a su necesidad, deben generarse mecanismos que permitan dicha acción, con el objetivo de optimizar la experiencia de uso.

- *Adaptación al hardware*

  Aunque habitualmente un CMS permite la interacción con el usuario a través de sus consolas multifunción, cabe la posibilidad de que las circunstancias determinen la conveniencia de utilizar distintas opciones de hardware para su ejecución. Características como el número de pantallas, la resolución de las mismas o incluso la ejecución en dispositivos alternativos como pantallas de gran formato o pequeñas tabletas, no deben impedir que el sistema de administración de combate ofrezca a los usuarios la totalidad de sus capacidades. Esto implica la capacidad de efectuarse correctamente con independencia del soporte en el que se haga.

- *Adaptación a los recursos*

  En este apartado, tomaremos en cuenta aspectos como el tipo de ejecución (centralizada o distribuida)

y el modelo de redundancia. El CMS debe ser capaz de adaptarse convenientemente a los recursos disponibles en cada momento, garantizando que las condiciones cambiantes en el mismo entorno de ejecución no afectarán al desempeño de la misión.

2.2 Escalabilidad[1]

La escalabilidad o extensibilidad es una medida de la capacidad de un sistema, para ser ampliado e indicar el nivel de esfuerzo requerido para implementar dichas extensiones; estas pueden consistir en la adición de nueva funcionalidad o la modificación de las ya existentes. La escalabilidad mide, de manera directa, la capacidad de crecimiento futuro de los sistemas de administración de combate.

Asimismo, existen distintas técnicas para organizar la facultad de crecimiento, las cuales son:

- **Caja blanca**

  El sistema *software* puede ampliarse modificando el código fuente. Es la técnica más flexible y la menos restrictiva. A su vez, podemos distinguir entre:

  - Los cambios se realizan de manera invasiva y el código fuente original se modifica directamente. Por otro lado, es la más relevante en la corrección de errores, la refactorización de código interno o la producción de la próxima versión del CMS.
  - Caja de cristal. Se le conoce también como *marco basado en la arquitectura*. Facilita la extensión con el código fuente disponible, pero sin permitir su modificación. Las extensiones deben separarse del sistema original, de manera que este no se vea afectado. Un ejemplo de esta forma de escalabilidad

NOTA

1 Aunque en inglés *scalability y extensibility* hacen referencia a diferentes conceptos, en este documento sus traducciones al español se utilizan como sinónimos, pues aunque es extensibilidad la palabra que mejor expresa la capacidad de crecimiento futuro de un sistema software, se pretende fijar la idea de que un CMS debe ser capaz de escalarse de manera adecuada a cualquier tipo de misión, de ahí que se prefiera, en ese contexto, usar ambos términos como intercambiables en español y en el ámbito de este trabajo.

son los marcos de aplicaciones orientadas a objetos que logran la extensibilidad típicamente mediante el uso de las técnicas de herencia y enlace dinámico.

- **Caja negra**

  También llamada *marco basado en datos*. Aquí no se utilizan detalles sobre la implementación del sistema para poner en funcionamiento las extensiones, dado que solo se proporcionan especificaciones de interfaz. En general, se logra mediante aplicaciones de configuración del sistema (o el uso de lenguajes de secuencias de comandos específicos de la aplicación) mediante la definición de las interfaces de los componentes.

  Lo habitual en un sistema tan complejo como un CMS es el uso de ambas técnicas, cada una de ellas aplicada a distintas partes del *software*. Esto es lo que se conoce como caja gris, la cual genera un compromiso entre la caja blanca y la caja negra. Por otro lado, no depende completamente de la exposición del código fuente, ya que los programadores reciben la interfaz de especialización del sistema que enumera todas las abstracciones disponibles para el refinamiento y especificaciones sobre cómo deben desarrollarse las extensiones.

  Desde el punto de vista del diseñador, el objetivo es que un mismo CMS sea capaz de adaptarse a distintos usuarios, es decir, a distintas marinas de guerra. Desde el punto de vista de los usuarios, en este caso la Marina, el objetivo último de la escalabilidad debe ser que un mismo CMS sea capaz de adaptarse a todos los tipos de buque (o al menos, todos los buques del mismo dominio). Ambos objetivos pueden lograrse si se tiene en cuenta el requisito de la extensibilidad desde el mismo instante en que se comienza a diseñar la arquitectura del sistema.

2.3 Mantenibilidad

Se le define como el grado de facilidad con el que un sistema puede ser mantenido, para corregir defectos, reparar o reemplazar ciertos componentes sin tener que suplir otros, prevenir condiciones de trabajo no anticipadas y, sobre todo, incorporar nuevos requisitos. La mantenibilidad es una de las ocho características del modelo de calidad del software definido en el estándar ISO/IEC 25010 *Quality model and guide*.

- **Corrección de defectos y ampliación de funcionalidad**

  El mantenimiento del *software*, definido como cualquier modificación hecha al código durante su desarrollo o después de su entrega, consume hasta el 90% del costo total de un proyecto de *software* típico. Agregar nuevas funcionalidades, detectar defectos de mantenimiento, corregirlos y modificar el código para mejorar su calidad son las principales actividades del esfuerzo de mantenimiento.

  Los sistemas navales de administración de combate tienen una vida media de entre 20 y 40 años, en relación a la vida del buque. Durante este tiempo, es frecuente que reciban actualizaciones tanto para la corrección de los defectos encontrados y reportados por los operadores, así como para la incorporación de nuevos requisitos: los sensores son reemplazados por nuevos sistemas, más prestantes o fáciles de mantener, nuevos actuadores se incorporan para ampliar las capacidades de la plataforma, aparece la necesidad de participar en escenarios de comunicación complejos que hace indispensable la integración de nuevos sistemas de enlace de datos, entre otras cuestiones. Las razones para que el *software* del CMS deba ser actualizado durante su vida útil son muy abundantes y consumirá un gran número de horas para estas actividades, a

menudo mayor que el tiempo invertido en el propio desarrollo del sistema.

Por todo ello, el retorno de la inversión, asociado a los esfuerzos para optimizar la mantenibilidad del sistema

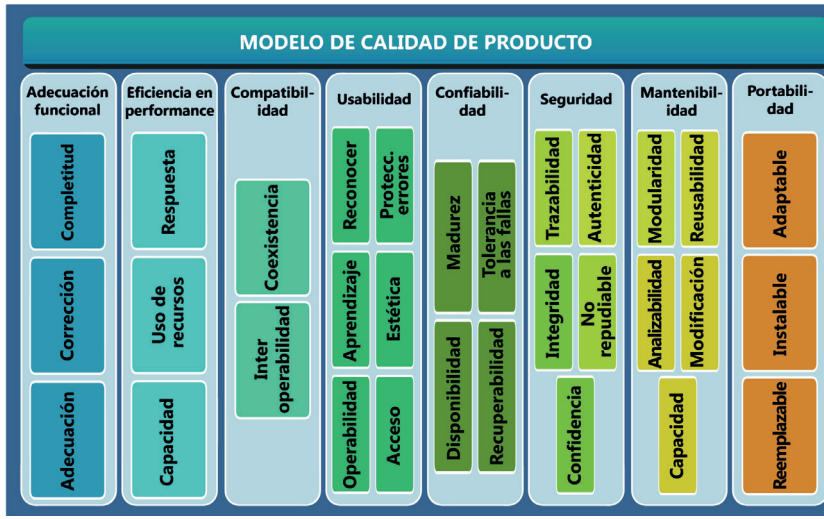


Figura 2: los ocho requisitos para la calidad de un sistema software según ISO 25010.
Fuente: expuesto por el autor.

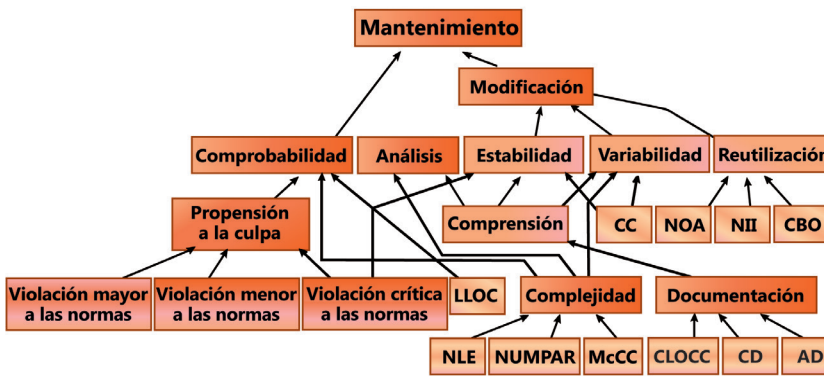


Figura 3: modelo de mantenibilidad ISO 25010.
Fuente: expuesto por el autor.

software, desde las primeras etapas de su diseño, será con toda seguridad elevado y justificado.

- **Resolución de obsolescencia**

  Un caso particular de mantenimiento, durante la vida de un CMS, es el relacionado con la resolución de la obsolescencia. La tendencia a utilizar componentes *Commercial of the shelf* en la fabricación del *hardware* de los sistemas, para maximizar el aprovechamiento del veloz avance de las tecnologías, conlleva la contrapartida de gestionar la obsolescencia de dichos componentes, que con toda probabilidad quedarán descontinuados por sus fabricantes en algún momento de la vida del CMS que los utiliza.

  Por tanto, es importante asumir que tendrán que llevarse a cabo, tarde o temprano, actividades de mantenimiento orientadas a resolver la obsolescencia del *hardware* o, incluso, del entorno operativo del sistema. Es evidente que toda inversión de esfuerzo orientada a promover una arquitectura que maximice el requisito de la mantenibilidad será percibida, con el tiempo, como una decisión inteligente.

3. Recomendaciones

3.1. Arquitectura objetivo de un sistema de administración de combate

Hasta ahora nos hemos esforzado por defender la necesidad de que un CMS disponga de una arquitectura que garantice su adaptabilidad y escalabilidad. Asimismo, se argumentó por qué este objetivo debe apoyarse en una revisión de los parámetros significativos para la arquitectura del sistema, incidiendo especialmente en tres de ellos.

En los próximos párrafos propondremos algunas claves para facilitar este objetivo, comenzando por la definición de la arquitectura a partir de criterios sencillos, como son la organización del *software* en un conjunto de

dominios funcionales, la clasificación de las capacidades en fundamentales y específicas, y la definición de los componentes *software* de cada uno de los dominios.

- **Dominios funcionales**

  Un sistema de administración de combate se caracteriza por su elevada complejidad, tanto en el abordaje de su desarrollo como en su mantenimiento futuro. Por ello, es recomendable su descomposición en elementos más sencillos y con ámbitos de aplicación acotados. Nuestra propuesta es establecer los siguientes dominios funcionales:

  - *Mando y control*

  Comprende fundamentalmente las capacidades relacionadas con la gestión de las amenazas, gestión de los distintos dominios *warfare* —antiaéreo (AAW), antisubmarino (ASW), antisuperficie (ASuW), asimétrico (ASyW) y guerra electrónica (EW)—, herramientas de apoyo a la decisión, y otras funciones de mando y control, como el control aéreo de aeronaves o el de desembarco anfibio.

  - *Gestión de información táctica*

  Son las capacidades de mantenimiento de la base de datos de trazas del sistema, incluyendo procesos de identificación, distribución de datos tácticos y, en definitiva, todos los que tienen por objetivo la generación de la *tactical picture*.

  - *Infraestructura*

  Este dominio se encarga de servicios tales como los de red, monitorización de nodos y procesos, distribución de datos, registro de datos, entre otros.

  - *Usuario*

  Los procesos relacionados con el soporte al usuario comprenden la gestión de roles del sistema, gestión

de alertas, acciones del operador, servicios y marcos de trabajo para aplicaciones de interfaz, figuras de operador, ventana de situación táctica y otras herramientas de visualización de información.

- *Gestión de sensores*

Referido a la responsabilidad de mantener el estado, la gestión y el control de los sensores del buque, además de la búsqueda, detección y seguimiento de blancos, y la transición de blancos a trazas.

- *Gestión de actuadores*

Función encargada de mantener el estado, la gestión y el control de los actuadores del buque, las órdenes de enfrentamiento, la selección de armas y el control de las hostilidades.

- *Gestión de comunicaciones*

Conforman este dominio los procesos relacionados con los equipos de comunicaciones externos, como los distintos tipos de enlaces tácticos de datos.

- *Gestión de vehículos*

El control de los vehículos no tripulados y sus cargas de pago caen bajo el alcance de este dominio funcional.

- *Buque*

En este dominio funcional se incluyen todos los procesos relacionados con la propia plataforma, como los servicios de navegación, distribución de datos meteorológicos o el horario.

- *Adiestramiento*

Una característica fundamental de los CMS modernos es la posibilidad de disponer de adiestramiento integrado. Este dominio incluye procesos como el controlador de escenarios de simulación, los propios simuladores de

sensores y armas o los servicios de gestión de modo de funcionamiento.

- **Capacidades «core» versus capacidades específicas de la plataforma y la marina**

  Cuando hablamos de que un CMS debe servir para cualquier misión, afirmamos que este es capaz de funcionar en varios tipos de plataforma. En base a ello, se dice que todo CMS debe disponer de características comunes a todas las configuraciones de cada plataforma donde se instala. La siguiente figura ilustra este punto:

  Se denominan capacidades «core» a aquellas que se consideran necesarias en todas las plataformas y a las facultades específicas de estas o de la Marina. Asimismo, se aplican en un determinado buque o para un usuario concreto, como podría ser el caso de la integración de un radar o del algoritmo que implementa una característica particular de la doctrina operativa de una marina de guerra.

  Como puede observarse, algunos dominios funcionales se consideran íntegramente incluidos en el grupo de capacidades «core». Este es el caso de la gestión de trazas, el mando y control[2], así como también la infraestructura. Por el contrario, la mayor parte de funciones disponen de una parte nuclear y otra específica; esta característica es precisamente la que permitirá implementar los mecanismos adecuados para disponer de un CMS capaz de ser utilizado en distintas misiones.

NOTA

2 Nótese que incluso ciertas capacidades de mando y control, que podrían en un principio caracterizarse como particulares de una plataforma, como es el caso de las mencionadas en el párrafo anterior en relación al control aéreo o el control de desembarco, aplicables solo en buques con un rol portaeronaves y anfibios, se consideran igualmente nucleares, es decir, componentes incluidos en la sección «core» del CMS.

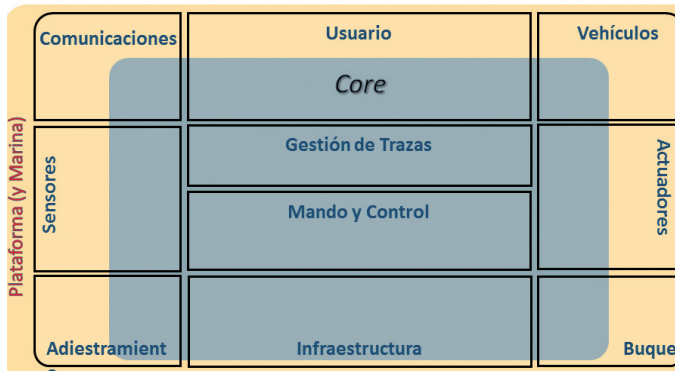


Figura 4: capacidades «core» versus capacidades específicas de la plataforma y la marina.
Fuente: expuesto por el autor.

- **Definición de componentes: servicios y aplicaciones tácticas**

  El paso final en la definición de la arquitectura del CMS, el cual permitirá alcanzar los niveles deseados de adaptabilidad, escalabilidad y mantenibilidad, es la distinción de los componentes *software* en dos tipos, servicios y aplicaciones, y su distribución en las zonas *core* o específica de los diferentes dominios. Este punto queda ilustrado en la figura 5.

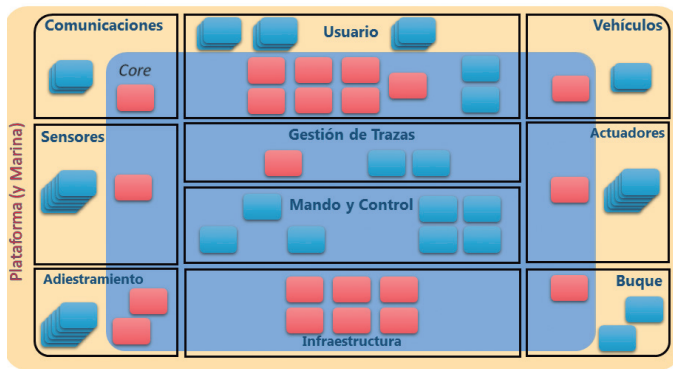


Figura 5: componentes software de tipo servicio y aplicación táctica.
Fuente: expuesto por el autor.

Como se observa en los ejemplos incluidos en la figura, todos los servicios se consideran «core», aunque sus componentes no son solo de tipo servicio, dado que entre ellos también encontraremos aplicaciones tácticas, como las que alojan la funcionalidad asociada a la gestión de las distintas *warfares*.

Es importante destacar que la presencia de los servicios gestores, con particular relevancia en el gestor de sensores y el de actuadores que aparecen en el ejemplo, pero también los equivalentes para la gestión de los sistemas de comunicaciones o vehículos, son los que facilitan la capacidad de crecimiento de la arquitectura. Esto es posible mediante la incorporación de componentes específicos que resuelven la interfaz con un sistema externo concreto, pues la responsabilidad de convertir los flujos de información (datos y control) de ese sistema externo al modelo interno del CMS recae sobre los servicios «core» de gestión, cuya presencia debe darse en todas las plataformas, independientemente de la configuración concreta de los sensores, actuadores, sistemas de comunicación y vehículos de la misma.

3.2. Otras recomendaciones

Aunque el conjunto de claves para la definición de la arquitectura más adecuada que hemos presentado en la sección precedente conforma la recomendación fundamental para maximizar los tres atributos discutidos en el segundo bloque de este análisis, no es la única que podemos proporcionar. En los siguientes párrafos se proponen otras de distinta naturaleza, pero de gran interés a nuestro juicio.

- **Uso de estándares**

  La alineación con estándares suele conllevar una cierta complejidad, debido a las restricciones que pueden generar o por los esfuerzos requeridos para

su aplicación. A pesar de ello, existen beneficios claramente perceptibles cuando se elige operar en función de lo que se establece en los estándares. La figura 6 resume los más destacados a juicio del autor.

Por otra parte, es importante distinguir entre los distintos tipos de estándares.

En tal sentido, la figura 7 ofrece una vista de los dos ejes fundamentales: estándares abiertos frente a los estándares cerrados, y estándares oficiales contra los estándares industriales.

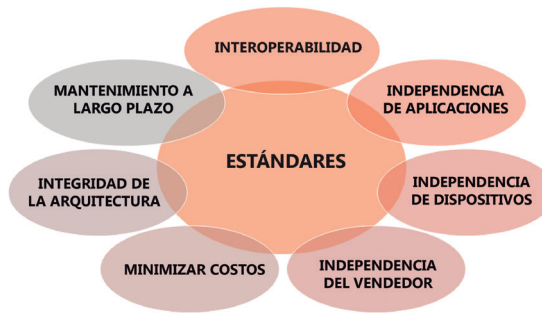


Figura 6: beneficios asociados al uso de estándares.
Fuente: expuesto por el autor.

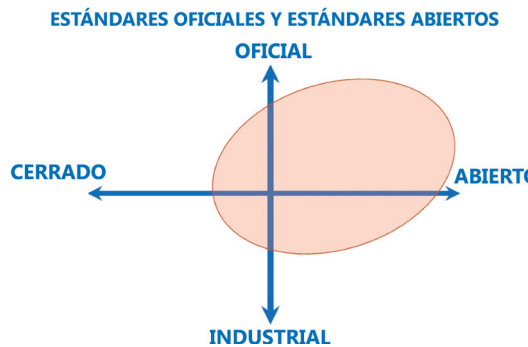


Figura 7: estándares oficiales y abiertos.
Fuente: expuesto por el autor.

Los estándares cerrados son exclusivos de un fabricante o vendedor y suelen estar disponibles solo bajo términos restrictivos establecidos en un contrato con la organización que posee el copyright de la especificación de ese estándar. Los estándares abiertos, por el contrario, son aquellos que se encuentran disponibles de manera pública

Por otro lado, se denomina estándares oficiales a los que mantienen una organización de estandarización, mientras que los estándares industriales, también llamados de facto, son aquellos establecidos por grupos de empresas y organizaciones, pero que aún no son oficiales.

El uso de unos u otros estará determinado por las necesidades del proyecto, siendo una cuestión que debe ser estudiada en cada caso concreto. No obstante, para mantener las ventajas resaltadas en los primeros párrafos de esta sección, en especial las relacionadas con la independencia, nuestra recomendación es maximizar el uso de los estándares oficiales y abiertos.

- **Patrones (y Antipatrones) de diseño**

  Los patrones de diseño son un conjunto de técnicas creadas para resolver problemas comunes en el desarrollo *software* y otros ámbitos referentes al diseño. Mediante el uso de estos, los diseñadores de un CMS (y de cualquier sistema software) tendrán acceso a las siguientes ventajas:

  - Catálogo de elementos reutilizables.
  - Soluciones a problemas ya conocidos.
  - Diseño estándar.
  - Vocabulario común con otros diseñadores.
  - Mayor facilidad en el aprendizaje.

En tanto, es posible encontrar patrones de muy diversas categorías que resuelven problemas de diferente naturaleza. De este modo, se dispone de patrones que facilitan la creación de instancias, solucionan problemas de estructura, ofrecen soluciones al comportamiento o resuelven la interacción con el operador.

La recomendación de los autores pasa por obtener un conocimiento profundo de los patrones de diseño que permita conocer la existencia de una solución ya probada y reutilizable (definición última de los patrones) que facilite la resolución de los problemas inherentes al desarrollo del CMS y estandarice su diseño, lo que sin duda redundará en acercarnos más a nuestra meta de crear sistemas de administración de combate con las máximas cotas de adaptabilidad y escalabilidad.

A menudo nos concentramos exclusivamente en los requisitos funcionales y no dejamos tiempo para vigilar otros aspectos importantes, pero es igualmente importante prestar atención a la posible aparición de los denominados antipatrones, que se definen como malos patrones de diseño que, invariablemente, nos llevarán a una mala solución; como los patrones son numerosos, el peligro principal radica en que los desarrolladores que los utilizan no son conscientes de ello, ya que creen estar aplicando la solución correcta a un problema cuando, en realidad, hacen lo contrario.

- **Metodología**

  El último punto cubierto en este apartado de recomendaciones es el de la metodología de desarrollo. Aunque parece un asunto fuera de lugar, en el ámbito que pretende cubrir el presente estudio, pensamos que su aparición en el mismo se justifica por una sencilla razón.

Cuando hablamos de sistemas *software*, nos centramos en aspectos tales como los requisitos funcionales y no funcionales, la arquitectura o su evolución futura, olvidando un aspecto absolutamente fundamental a nuestro juicio: el factor humano.

Los CMS son desarrollados por equipos de personas cuya organización y metodología de trabajo tendrán influencia directa tanto en el grado de éxito alcanzado en la consecución de los objetivos (en este caso el de maximizar la adaptabilidad y escalabilidad del sistema) como en la calidad final del producto.

En cualquier caso, más que utlizar una u otra metodología de desarrollo, la intención del autor es recordar la necesidad de otorgar a esta cuestión la importancia que merece y tomar la decisión con anterioridad al proceso de diseño de la arquitectura del CMS.

En términos generales, podemos distinguir entre dos grandes tendencias: el desarrollo tradicional y el desarrollo ágil. Ambos tienen ventajas e inconvenientes y son más adecuados para unas u otras situaciones; por un lado, el desarrollo tradicional se orienta a la planificación y fijación de requisitos de manera rígida, estimando el coste y el tiempo que se empleará para la implementación de los mismos.

Por el contrario, las metodologías denominadas ágiles mantienen fijos el tiempo y el coste, especializándose en aportar valor al sistema con cada iteración del desarrollo, por lo que estas capacidades son tomadas en cuenta desde el inicio.

La figura 8, referida al enfrentamiento entre la metodología tradicional y la metodología ágil, ofrece de manera gráfica lo que acabamos de exponer.

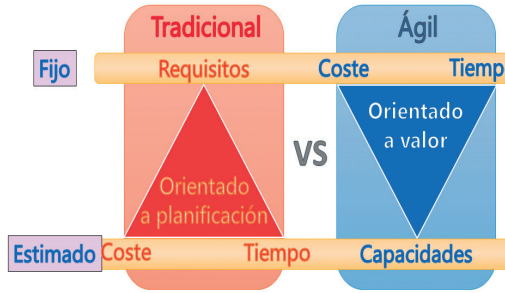


Figura 8: metodología tradicional versus metodología ágil.
Fuente: expuesto por el autor.

4. Conclusión

A modo de resumen, queremos ofrecer a continuación las principales conclusiones del presente trabajo:

1. Un sistema de administración de combate es, esencialmente, un sistema *software* y debe ser tratado como tal.
2. Los requisitos no funcionales de adaptabilidad, escalabilidad y mantenibilidad son esenciales para optimizar la vida útil de un CMS.
3. Por lo general, un sistema de administración de combate debe adaptarse al usuario, el entorno, la misión y los nuevos requisitos.
4. El diseño la arquitectura del sistema es fundamental para la optimización de la vida útil del sistema. El reparto de capacidades en dominios funcionales y la orientación a servicios pueden ayudar a lograrlo.
5. No deben descuidarse otras consideraciones de gran importancia, como el uso de estándares, la aplicación de los patrones de diseño más adecuados y la metodología a utilizar en el proyecto.

5. Agradecimiento

Muestro una vez más mi agradecimiento a la Escuela Superior de Guerra Naval de la Marina de Guerra del Perú, por su cordial invitación a participar en el V Simposio de Internacional de Seguridad y Defensa.

Referencias

Chen, L. Abar, M. & Nuseibeh, B. (2013), *Characterizing architecturally significant requirements*. Recuperado el 6 de agosto de 2019 de https://ulir.ul.ie/handle/10344/3061

Mancera Araujo, D. (setiembre de 2019), *Asegurando un alto nivel de adaptabilidad y escalabilidad en los sistemas de administración de combate modernos*. En el V Simposio de Seguridad y Defensa llevado a cabo en Lima, Perú.

sesión

3.1

Innovación tecnológica en los buques de la Armada Española: ejemplo de éxito en el sistema de combate de la armada

Valm.
Manuel Antonio Martínez Ruiz

Quiero agradecer a la Armada del Perú por haberme invitado a este simposio, para dar a conocer esta ponencia, la cual pretendo derivar hacia la práctica tras revisar algunos aspectos teóricos.

Ustedes se preguntarán qué hemos hecho en la Armada durante los últimos 30 o 35 años. Lógicamente, el foco de atención estará direccionado hacia los productos recientes, los cuales han sido desarrollados en conjunto con la Armada de España, el Ministerio de Defensa y el Estado Español. Cabe mencionarles que el Gobierno ha decidido poseer ciertas capacidades críticas en favor de la industria nacional y de la soberanía tecnológica en general.

En primer lugar, definiré qué es un programa de éxito. Hace algunos años, teníamos diseños importados, en contraparte a las construcciones que se ejecutaban en España. Es costumbre de los españoles confiar en los astilleros nacionales, como es el caso de la sociedad pública Navantia; esta sociedad de construcción naval fue formada por ingenieros de la Armada y, posteriormente, se separó del sector castrense. Hoy en día, Navantia forma parte del grupo de empresas del sector público vinculadas al Estado. Debido a su separación de la Armada, las responsabilidades y actividades se desarrollan en campos distintos.

En tal sentido, la Armada de España tiene la responsabilidad de definir qué es lo que se requiere en la institución y formular los requisitos para obtener el producto deseado. Una vez planificados estos puntos, es nuestro deber exigir a las empresas la entrega de los productos y sistemas que requerimos. Con ello, no solo me refiero a Navantia como autoridad del diseño, sino a todas las empresas de nuestro entorno.

En base a esto, hemos pasado por un proceso evolutivo en el transcurso de los años, tanto en la línea de submarinos, fragatas —quizás sean las que han sufrido mayores

variaciones— y otros buques. Este hecho generó un interesante viraje: de poseer modelos de diseño importado y construcción nacional, pasamos a tener modelos de diseño nacional, construidos en territorio nacional y con calidad de exportación.

Es preciso tener en cuenta que, cuando hablo de buques, estoy haciendo alusión a sistemas; el buque de guerra no es una plataforma, sino un sistema que posee un soporte y una carga de pago, conformado por los sensores, las armas, la logística y la habitabilidad. Asimismo, es un sistema que posee autonomía logística y, por lo tanto, la integración correcta de sus partes será el objetivo final de una serie de requisitos.

Este modelo tiene una réplica en el sistema de combate. Antes de definir dicho punto, quiero mencionarles que recientemente tuvimos en Madrid unas jornadas de trabajo con la Armada de España, las cuales fueron patrocinadas por una serie de instituciones y la industria; este evento nos hizo pensar en lo que podrían ser los buques y fragatas de la nueva generación. Una vez obtenida la firma del Gobierno en el contrato de las fragatas F110 y cuando empecemos con el desarrollo del diseño del programa, podremos decir que vamos encaminados a nuestro objetivo. Por el momento, resulta osado hablar de la construcción de buques sofisticados. Y, ¿por qué decimos que estamos "pensando" en estas naves? La respuesta es sencilla: entre una hoja en blanco y un sistema entregado a la Armada transcurren entre quince o veinte años.

Es necesario pensar detenidamente en estos proyectos, ya que sería un despropósito no hacerlo. Esta proyección permite la visualización del entorno geoestratégico y del momento en que los futuros buques entrarán en servicio (posiblemente estemos hablando del año 2035 o el 2040). En ese entonces, el entorno geoestratégico será distinto al actual y las amenazas serán diferentes. Por tal motivo, es

necesaria la construcción de sistemas que hagan frente a los peligros del futuro.

Por otro lado, es preciso reflexionar respecto a la transición de la hoja en blanco a la construcción de un buque, así como también en el énfasis que debe ponerse en la elaboración del concepto de un proyecto. Lo más importante en este sistema es establecer los pilares de los requerimientos.

Ejemplo de esta premisa es la fragata F110, la cual se entregará en el 2026, pero cuya concepción rondaba nuestras mentes en el 2010. De hecho, es importante que destinemos esfuerzos suficientes para desarrollar un óptimo estudio de factibilidad. Es aquí cuando empieza la fase conceptual de viabilidad, lo que se traduce en la generación del llamado DNO (Documento de Necesidad Operativa). En ese sentido, nuestros procesos de construcción se rigen bajo la metodología establecida por la OTAN, plataforma donde se encuentra insertada la fase conceptual junto con las de diseño, ejecución y entrada en servicio.

Dichas etapas deben recibir el mayor cuidado posible en sus ejecuciones, siendo la fase conceptual la de mayor relevancia. Si trabajamos esta etapa de manera óptima, acertaremos en las demás partes del proceso. En el caso de España, somos un país que no puede permitirse el lujo de fallar —aunque hay ocasiones en que los errores generan mejoras en los sistemas, pero son situaciones *sui generis*—.

Esto sucede en el caso de la F110, la cual recolecta los aspectos específicos de un programa naval como la transparencia; es necesario, además, profundizar en el conocimiento intrínseco de la Armada, ya que dicho saber no puede externalizarse.

En tal sentido, la Armada debe conocer al detalle el producto que recibirá. Esto es lo que nosotros conocemos como *engineering agent*, en el caso de la experiencia,

mientras que, por el lado de los sistemas de combate, lo denominamos *Combat System Engineering Agent*. En esto concluimos que la responsabilidad de un proyecto no puede ser distribuida.

Desde los orígenes de este modelo de éxito, una serie de compañías estratégicas, junto con el Ministerio de Defensa de España y la Dirección General de Armamento y Material, han apostado por mantenerlo vigente. Estas entidades empezaron sus operaciones con sistemas muy modestos, los cuales fueron creciendo y hoy en día son capaces de exportar productos con un nivel de excelencia comprobada. Precisamente, estas empresas nos entregan y desarrollan los sistemas que requerimos.

Como bien se mencionó en este estrado, la ingeniería de sistemas aplicada al desarrollo no puede utilizar sistemas caóticos sin el debido control, hecho que exige a la industria maximizar y optimizar sus procesos.

La exigencia hacia las empresas con las que trabajamos —como Navantia Sistemas— radica en que se adopten estándares de ingeniería de sistemas en cada proyecto. En el caso de los submarinos, estos pertenecen a un estándar distinto a diferencia de los buques de superficie, pero el rigor en sus desarrollos es absoluto tanto en el proceso de construcción, en la ejecución de pruebas y la trazabilidad de los requisitos. Actualmente, hemos apostado por el Sistema de Combate (SCOMBA) como el único sistema de los buques de la Armada Española.

De igual modo, nos interesan otros temas de gran relevancia como el proceso de automatización de nuestros astilleros y de la industria 4.0; la maximización del apoyo logístico supone también otro objetivo a conseguir, por ello, es necesario realizar actividades de mantenimiento preventivo en lugar de acciones predictivas, echando mano de las nuevas tecnologías a nivel de la ingeniería de sistemas. No olvidemos que es importante buscar al socio tecnológico adecuado para llevar a cabo nuestros proyectos.

Es evidente que somos capaces de hacer muchas cosas. En España, la industria nacional es buena en distintos campos, pero no abarca la totalidad de los requerimientos. En consecuencia, es necesario encontrar a un socio tecnológico adecuado para el correcto desarrollo de un proyecto; una vez seleccionado, deben celebrarse acuerdos de cooperación industrial que posibiliten la fabricación de los buques de la siguiente generación en suelo español.

Este hecho brinda una dosis de soberanía estratégica. En la actualidad, gracias al modelo vigente, España es capaz de producir un buque de guerra, diseñar sensores, sistemas, el control de plataformas — que es tan importante como el sistema de combate y la integración de armas— y apoyar en el ciclo de vida. Esto simboliza la concretización de los acuerdos y demuestra un método de trabajo que une la parte industrial con el ámbito de la Defensa y el campo de la Armada, enlazado a su usuario final.

Figura I: Soberanía estratégica.
Fuente: expuesto por el autor.

Permítanme enfatizar cuan necesaria es la industria para nosotros. No podríamos seguir la línea actual, en cuanto a los modelos de desarrollo establecidos, si no tuviésemos

una industria que apueste por nosotros y viceversa. Esto refiere lo que popularmente se conoce en los negocios como un *win to win*; tanto la industria, la Armada y los usuarios finales debemos estar sintonizados, ya que la industria necesita apoyo institucional y requiere de investigación, desarrollo e innovación (proceso conocido como I+D+I). Por ejemplo, para mantener la cartera de pedidos es necesario brindar soporte en lo referente al ciclo de vida. Si pensamos adquirir una generación de fragatas no sólo habría que pensar en los buques, sino también en sus respectivos ciclos de vida y los costos.

Veámoslo de esta manera: una persona compra un Ferrari a un precio bajo, pero luego le resulta imposible echarle gasolina. Pasado un tiempo, se le pincha una rueda y no puede cambiarla porque dicha acción es costosa. Tengan por seguro que el Ferrari terminará guardado en el garaje de este hombre, mientras va en busca de un Prius (que es lo que debió hacer desde el principio). Lo mismo sucede en el campo de la industria: se puede desear cualquier vehículo de última generación, pero es necesario ser realistas en cuanto a los requisitos y detallar minuciosamente lo que se desea obtener.

A continuación, pasaremos a revisar lo concerniente a un sistema de combate. Mi compañero disertó respecto a la parte del sistema de gestión de combate, por lo que pondré énfasis en lo que significará este trabajo en la fragata F110 Spider Chart. Una forma gráfica de describirlo sería señalar que en la parte izquierda se ubicarán los sensores; en la parte central encontraremos los procesos y en el lado derecho las armas. El CMS se ubicará en la zona de procesos, mientras que el SCOMBA se encargará de gestionar las interfaces de todos los sensores y armas, utilizando para ello requisitos de operación en tiempo real dependientes de la función táctica.

Desde el principio, hemos apoyado en España el proceso para obtener la parte CMS común, con versiones que se

adapten a distintos tipos de barcos, ya que es diferente hablar de un submarino, de una fragata o de un buque de acción marítima. Sin embargo, las funciones, arquitectura y mantenimiento son iguales en los tres casos. Me permito tomar este punto, a modo de contexto, con el fin de clarificar a que parte del Spider Chart me refiero.

Anteriormente, los sistemas de combate de la Armada eran entes dispersos, en lugar de plataformas. Esto nos llevó a una situación logística descabellada, pues cada sistema tenía su propia plataforma tecnológica, sus desarrolladores y sus lenguajes de programación. Debido a estas variaciones, resultaba imposible unificarlas y optimizar el mantenimiento del sistema de combate.

Es por ello que, a partir del año dos mil, se decidió utilizar un núcleo de transferencia de tecnología proveniente de los trabajos realizados en las fragatas F100 y FR90; concretamente, esto vino de un núcleo de transferencia tecnológica de la parte AEGIS, con Lockheed Martin y la Marina Americana. A partir de ese núcleo empezó nuestro crecimiento, sobre todo en cuestiones metodológicas, por encima de otras funciones similares. Durante veinte años, casi todo lo controlado por el sistema de combate, en distintos buques de la Armada, fue creado por un equipo de trabajo en Navantia Sistemas, institución a la cual confiamos los desarrollos de nuestros requisitos específicos. En base a ello, se han desarrollado las distintas versiones del sistema de combate SCOMBA, hasta llegar a la F110.

En cada versión asumimos diversas responsabilidades en cuanto a navegación, gestión de trazas, vinculación, responsabilidad de engagement y gestión de armas hasta que, como señalara mi compañero Juan Carlos, la F110 fue nacionalizada en un 90%, restando solo la parte de gestión de misiles SM2. Esta parte se encuentra integrada con piezas de elaboración nacional, que llevan el sello de

Lockheed Martin. Esto fue posible gracias a una apuesta específica de España y de la Armada por el modelo.

Permítanme relatarles cómo surgió esta iniciativa. En un inicio, contábamos con una serie de buques y diseñábamos distintas versiones del SCOMBA, sistema creado para buques diferentes a las fragatas, a las naves de acción marítima, a los LHD y a los buques logísticos. Debido al éxito en su desarrollo, se introdujo el SCOMBA en los buques de acción marítima, que son estructuras más complejas y poseedoras de múltiples funciones, mientras se trabajaba en lo que sería el programa F100.

Dicha iniciativa sirvió para cimentar las bases del programa F105 y del F110. Por ello, estamos llegando a un punto en el que concurrirán los desarrollos específicos de fragatas AEGIS en el proyecto F110, sucediendo lo mismo con el desarrollo del SCOMBA, que continúa presente en el resto de los buques de la Armada. A partir de este punto seguiremos el curso de la línea base del SCOMBA, olvidándonos definitivamente del *spin-off*, para desarrollar un software flexible y adaptable a distintos requisitos y funciones.

Esto no significa que dicho programa sea un *plug and play*. Si alguien se los dijese de esta forma, no lo crean; conseguida la adaptación, es necesario pasar por un periodo de pruebas. Quizás se realicen modificaciones al trabajo, pero el concepto guía será siempre la obtención de la máxima funcionalidad en los demás buques de la Armada. Como mencioné anteriormente, al hablar de metodología me refiero a la clarificación de requisitos por parte de la Armada en la fase funcional, los cuales deberán elaborarse en el astillero constructor.

A propósito, estoy seguro que ustedes pensarán que la unión entre el astillero, la empresa y el proceso de ingeniería puede desencadenar acciones contaminantes. Les aseguro que esto no es así, debido a que poseemos

un alto sentido de la responsabilidad a nivel de los estados mayores y la ingeniería de la Armada. En este caso, se efectúa un proceso de reingeniería de requisitos para asegurar su cumplimiento.

Durante el proceso de evaluación de los requisitos en el árbol de especificaciones, notaremos la importancia de que un proyecto pueda llevarse a cabo en diez puntos específicos y en un determinado nivel. De este modo, se comprobará si el requisito es cumplible, trazable y sensible a ser probado; por eso, esta fase es fundamental, ya que el resto de etapas, llamadas *top-down* en esta rama y *bottom-up* en otra, aseguran los distintos niveles de representación de un sistema de combate. Asimismo, se garantiza que, a nivel *Preliminary Design Review* (PDR) y *Critical Design Review* (CDR), todos los requisitos establecidos serán desarrollados en base a una metodología puntual.

Cada hito posee criterios de entrada y salida, y se consideran culminados solo si el cliente los aprueba. En este caso, la Armada de España desempeña dicho rol, aunque las oficinas del programa se encuentran en la Dirección General de Armamento y Material. Nosotros trabajamos en conjunto con el objetivo de generar una óptima gestión del programa.

Esta parte corresponde a la fase de ejecución, que es tan importante como la etapa de pruebas, ya que cada una debe desarrollarse en un nivel de resolución vinculado a los requerimientos del cliente. Esto significa que un determinado nivel de requisitos específicos debe ser probado, con el fin de demostrar su presencia dentro de una jerarquía top down.

Lo que se hace aquí es probar elementos más pequeños en base a unidades de componente, para verificar la comunicación existente a nivel multielemento, siguiendo en dirección ascendente hacia la arquitectura del software. En cuanto a este último punto, es necesario realizar

pruebas exhaustivas y de manera jerárquica, para obtener la entrega final y la calificación operativa del sistema.

En ese sentido, nosotros hacemos los ensayos pertinentes en la Armada y las contrastamos con los requisitos del Estado Mayor, mientras que las pruebas de aceptación del sistema se corroboran con las especificaciones. En tanto, los test de afectación del sistema son brindados por el contratista para el cual hemos desarrollado los detalles. La única condición en este proceso es que el usuario quede conforme en cuanto al cumplimiento de sus requisitos. Como verán, lo sustancial no son los números, sino la posesión de un núcleo común de funciones del SCOMBA.

Durante todos estos años, se han efectuado más de doscientas mil especificaciones y 25 millones de líneas de código en distintos elementos y versiones del sistema de combate. Esto quiere decir que el éxito radica en detallar minuciosamente lo que se desea obtener; una vez definido el requerimiento, dicha acción fluye hacia abajo, comprometiendo a las demás funciones y generando una especie de transversalidad entre ellas. En algunos casos se cumplen todas y en otros solo unas cuantas, todo depende de la ambición que se tenga respecto al proyecto. Esto evidencia un punto importante: es mucho más fácil hacer el mantenimiento de un sistema en un punto determinado ya que si se optimiza, automáticamente lo harán todos los barcos.

Esta es una de las razones por las que la transversalidad funcional se convierte en un modelo de desarrollo exitoso. Cuando se pretende elaborar un sistema de combate, lo primero que debe hacerse es detallarlo. En principio, contábamos solo con requisitos dispersos y especificaciones de cierto nivel que, al ir descendiendo en el árbol jerárquico, generaron 250 mil especificaciones en el nivel más bajo, tal como mencioné anteriormente. Lo esencial es que estas acciones generen trazabilidad debido a que si una de las especificaciones cambia por

alguna razón, será necesario identificar si el causante de la afectación es un requisito de rango superior o inferior. En cuanto a las herramientas empleadas en el proceso, Navantia se encuentra inmersa en la trasformación digital de sus mecanismos, utilizando para ello herramientas específicas que producirán un cambio importante y paradigmático en la gestión de esta complejidad.

A continuación, pasemos a hablar de la descomposición funcional. Anteriormente, mi compañero habló de los sistemas afectados en cada una de sus partes. Esto ocurre en el sector de trazas y en la ubicación interna. Cabe mencionar que es importante tener en cuenta los requisitos y misiones, pues son elementos funcionales de un sistema de combate, junto con los requisitos cibernéticos. Respecto a este último punto, no podemos pensar en el desarrollo de sistemas de combate de última generación sin tener identificados esta clase de requerimientos.

El diagrama de contexto del programa F110 presenta una suite de sensores nacionales y un preprocesador de data links (enlaces de datos) relacionados a los vínculos 11, 16, 22, VMF, JRE, JRAP, en suma, todos los links para las operaciones de un barco que entrará en servicio a partir del año 2026. Estos vínculos de banda ancha serán integrados dentro del sistema de combate.

Por otro lado, este sistema cuenta con diversos servidores y consolas —todas de fabricación nacional— que representan las funciones y aplicaciones tácticas. Asimismo, cuando hablo de requisitos de ciberseguridad, me refiero a aquellos que afectan la gestión de riesgos y a la ingeniería de seguridad. Durante la jornada de ayer, se habló de la ciberseguridad en el campo de la defensa, así como de los controles de seguridad en la implementación de ciertas funciones y la compensación entre una excesiva seguridad y la falta de funcionalidad. Tomando este último punto, es necesario aplicar todos estos requisitos de forma coherente, si deseamos cumplir con los requisitos

cibernéticos escritos en el Estado Mayor del buque; de no hacerlo, podríamos ganar mucho por un lado, pero perder por el otro. Por lo tanto, es necesario obtener equilibrio y visualizar la compensación que se genera entre los impactos, riesgos y la seguridad frente a las capacidades.

De no cumplirse las condiciones, ¿cuáles serían son los sistemas afectados? Desde luego, el sistema de combate sería uno de ellos, pero las fuentes de entrada y de salida de información también sufrirían la afectación, ya que estamos hablando de un buque conectado entre sí. Recordemos que los buques forman parte de una red conectada, en tal sentido, tendremos las F110 junto a las F100 y a buques de la alianza con los de otros países, así como aviones Eurofighter y aviones F18, destacando por encima de estos el futuro avión de combate FCAS, el cual será desarrollado en veinte años junto con la F120, que desarrollaremos en ese mismo periodo. De alguna forma, un buque es un nodo conectado con el resto del mundo y precisamente en esa conexión estriba su vulnerabilidad.

Por otro lado. suena bien hablar del “internet de las cosas” y de las redes 5G, pues son tecnologías que posibilitan nuevas funcionalidades, sin embargo, imprimen un alto nivel de vulnerabilidad en los sistemas. Por ello, los requisitos de ciberseguridad que debemos tener en cuenta en esta situación residen en el establecimiento del equilibro tecnológico, que puede ser facilitador o elemento de vulnerabilidad.

Los elementos afectados son los RF2 de origen nacional, los de coalición, la red de sistemas integrados de plataforma, la red WAN PG y todas las redes. Nuestros buques no tienen un sistema de comunicación interior, en cambio, poseen diversas redes que cumplen una función específica. Los nudos de entrada y salida de esa red provienen de comunicaciones satelitales, convencionales, de comunicaciones IP, concluyendo con los data links y las comunicaciones para funciones especiales, a través de redes 5G, UVSAT, entre otras.

Lo mencionado hasta aquí son los sistemas afectados. Esto corresponde al requisito SICIB 08, habiendo otras siete líneas de requisitos cibernéticos que afectan al desarrollo de las F110; eso significa que no hemos olvidado el aspecto cibernético, por el contrario, es un sector fundamental que debe estar integrado al sistema de combate y no solo al de control de plataformas. Estoy seguro que ninguno de los presentes desearía que algún agente externo maneje a su antojo las turbinas de gas del barco, el sistema de comunicaciones o el de navegación.

En ese sentido, ayer se habló también que el spoofing podía hackear sistemas GPS. Por ejemplo, un barco puede tener un sistema GPS de última generación y una óptima hibridación para la navegación, sin embargo, es importante entender que, aún con todo ello, existen amenazas latentes.

La implementación de los requisitos cibernéticos conlleva a una serie de capacidades más avanzadas que otras. En la red multiservicios, por ejemplo, así como en el sistema de combate y la parte C2, hay piezas más protegidas que otras, existiendo un equilibrio entre la implementación del requisito y la funcionalidad propia.

En el caso de los enlaces de datos, estos posibilitan la comunicación entre dos sistemas de combate; además, corresponde al lenguaje de estos sistemas y cuando hablamos de su implementación, como el link 16, nos referimos a los programas que poseen todos los barcos tipo fragatas. Esto asegura que la mission computer del Eurofighter y del F18 se comuniquen con el sistema de combate del buque y cumplan una función específica. Entonces, un sistema de combate sin el pertinente enlace de datos es un programa que se mira en un espejo, encontrándose aislado y sin la posibilidad de cumplir con la función de conectividad.

Por fortuna, en España se apostó, desde 1995 o incluso antes, por este tipo de sistemas funcionales. Asimismo,

contamos con empresas que elaboran preprocesadores de data link; también participamos en programas internacionales de data link 16 y link 22, tenemos implementaciones VMF y JRE en nuestros buques principales, y somos autónomos en la integración de los enlaces de información con el sistema de combate. Algo que me consta, y sé que a ustedes también, es que poseen diversos sistemas de data links, pues tuve la oportunidad de verlo en Colombia hace unos meses y me pareció impresionante la autonomía estratégica que han conseguido.

En cuanto a las pruebas específicas del software del sistema de combate, el proceso inicia con la elaboración de un demo del mismo, como si fuese definitivo (con todos los sensores e interfaces entregadas a la Armada).

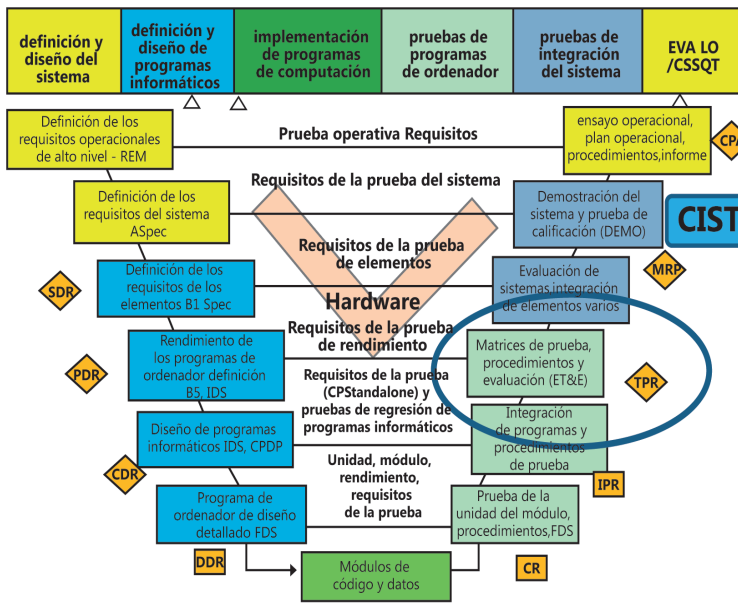


Figura 2: Metodología SCOMBA en V.
Fuente: expuesto por el autor.

Es importante entender que, si fallamos en las pruebas, lo haremos también en el sistema y bien sabemos que lo que no se prueba termina fallando. Esto es una verdad absoluta.

En tal sentido, para probar el software, los sensores y las armas del programa F110, hemos desarrollado una estructura dentro del SCOMBA que le permita a nuestros sensores tener una posición similar al barco; esto evidenciará si se encuentran debidamente integrados con el sistema de combate. Cabe preguntarnos por qué procedimos de esta manera: porque en el programa F105 tuvimos problemas con la reutilización al momento de integrar el radar *Spy* con el sistema de combate. La solución a este inconveniente fue utilizar una variante del radar.

Una de estas fue un simulador de interface que reconoció la integración óptima entre las mismas, pero cuando empezamos el proceso de integración a través de radiofrecuencias, saltaron a la vista otras cosas, por lo que tuvimos que hacer un esfuerzo adicional para subsanar la situación.

Hasta aquí, realizamos las pruebas de radiofrecuencia, pero no fue sino hasta que lanzamos el multibeam (ecosonda multihaz) que iniciamos con la integración de las partes. Debido a la presencia de muchos sistemas nuevos, fue necesario el desarrollo de una infraestructura que ayudase a caracterizar los sistemas a niveles de la TRL8 y TRL9, que suponen el nivel de madurez tecnológica de los desarrollos para sus respectivos despliegues. Una vez testeados, serán enviados a los buques.

Este es el primer prototipo, el resto fue implementado con las respectivas correcciones, pero esto lo dejaremos de lado, pues el ciclo de vida de los sistemas hace que las cosas cambien tanto en los SCOMBA como en los sensores. Por lo mismo, el entorno de pruebas del TRL8 tendrá suma relevancia en cuanto a sus contramedidas frente a

buques reales y aviones con todo tipo de elementos. Esto será instalado en la Base Naval de Rota, donde tenemos suficientes blancos para realizar las pruebas.

Otra cosa que estamos haciendo, y que afecta al desarrollo y a la concesión del sistema de combate, es el gemelo digital inserto en el contrato. Esto fue comentado ayer por el representante de Navantia; lo que queremos es tener una réplica digitalizada del buque para llevar a cabo diversas acciones, pero sobre todo, para hacer mantenimiento predictivo y desarrollar sensores que tengan un *Smartbyte* capaz de anticipar problemas que, de otra forma, serian difíciles de visualizar. Hoy en día, estamos produciendo sensores tipo Sierra, de control, en banda X y en base al sistema IRST para la detección pasiva de misiles y el sistema IFF Mod 5.

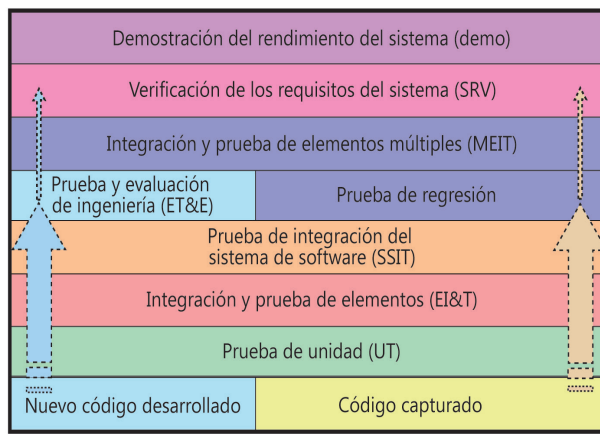


Figura 3: Metodología de pruebas.
Fuente: expuesto por el autor.

Este desarrollo empezó cinco años antes que firmásemos el contrato del banco, hasta que la CDR dio luz verde para que todos esos sistemas vayan a bordo, por lo que conseguimos un equilibrio basado en la innovación y la

creatividad. Debo confesarles que, por nuestra parte, la creatividad nos da un poco de miedo, a Navantia, un poco menos. Sin embargo, es cierto que en base a la tecnología e innovación seremos capaces de integrar sistemas probados a nivel TRL7, las mismas que pasan por el simulador TRL8 y el TRL9 colocados abordo.

Estos programas se mantienen gracias a la industria nacional, con el apoyo de socios tecnológicos *ad hoc*, que integran las tecnologías en esos sistemas, sobre los cuales disertará mañana el doctor Félix Pérez. Las tecnologías se encuentran a nivel Array en cuanto a su digitalización, estado sólido y apuntamiento en banda ancha digital. Los radares son planos, no hay antena ni nada que gire en el barco, solo los instrumentos de gestión que trabajan a través de los sistemas inteligentes del informe. Todo eso es integrado posteriormente en el sistema de combate y en las redes normales de IRST que provienen del Eurofighter adaptado para el entorno naval en el uso de formas de ondas importantes, para los nuevos desarrollos de los sistemas de radares 4.0.

Un ejemplo de esto es el radar Spy de estado sólido y otros equipos desarrollados. Después de muchos años, nos damos el lujo de fabricar partes críticas, cuando antes les teníamos miedo. Éramos creativos, pero temerosos en cuanto al abordaje de este tipo de tecnologías. Hoy en día, tomamos responsabilidad en ello.

A nosotros nos importa fabricar los barcos en los astilleros españoles, pero lo que más interesa es lograr que la industria gané experiencia en el desarrollo de tecnologías críticas y eso solo se conseguirá a base de acuerdos de cooperación industrial con las empresas que las producen. Este es el convenio suscrito con Lookheed Martin, quienes poseen suites de radares instalados en nuestros barcos.

No solo queremos que el sistema de combate sea nacional, sino también los sensores y por eso hacemos este

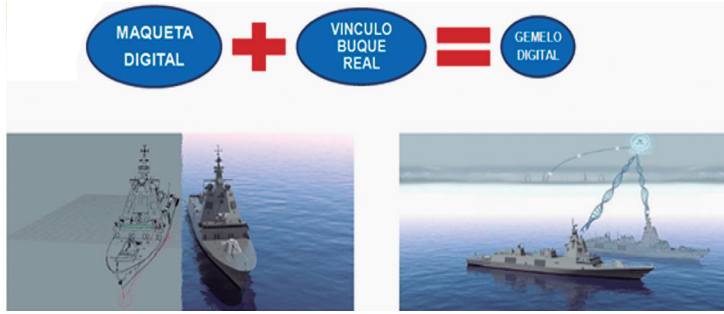


Figura 4: Tecnología de desarrollo naval.
Fuente: expuesto por el autor.

esfuerzo a nivel del radar banda Sierra (que es el sistema más importante del barco) pues funge como sensor de misiles y se le aplica toda la tecnología critica del programa F110. Asimismo, supone una parte importante del sistema de combate, pero es necesario resaltar que no configura un CMS, pues es la parte central del proceso y todo lo que esté dentro de la sipder chart es un sistema de combate.

Entonces, el CMS tiene que adaptarse a la particularidad de los sensores y estos deben ser capaces de tener una interface perfectamente identificada para ser negociada con las empresas y sensoristas, con el fin de que sea aprobada. Una vez conseguida su validación, vendrá la firma y la interface pasará a ser especificada, con el fin de utilizarse en el campo de la ingeniería.

El IRST, considerado dentro del top side del buque y donde irán cada uno de los elementos, es una novedad en la nave. Este reemplazó a las armas de pequeño calibre por las llamadas Sentinel 30 y 12,7 fabricadas por la empresa española Escribano Enginieering. Nuestros buques tendrán este tipo de armas, tal como otros barcos de la Armada que mantienen este requisito.

A modo de colofón, me queda confirmarles que destinar recursos en Defensa no es un gasto, sino una inversión que produce réditos y beneficios a nivel nacional, tanto

en las regiones donde esté implantada como en toda la estructura. Esta acción es conocida como la capilarización de todas las empresas que aportan al proceso de desarrollo. Un programa naval, aeronáutico o del ejército de tierra no supone un gasto: tengamos en cuenta los datos proporcionados por Navantia, aunque también serán válidas si provienen de cualquier otra empresa.

Las banderas del material español se encuentran en el S-80, en las F110, en el sistema de combate y en el buque. Mientras más banderas españolas haya, mejor para nosotros. Sin embargo, para no incurrir en errores, necesitamos socios tecnológicos fiables, con buenas referencias y dispuestos a apostar por la industria nacional.

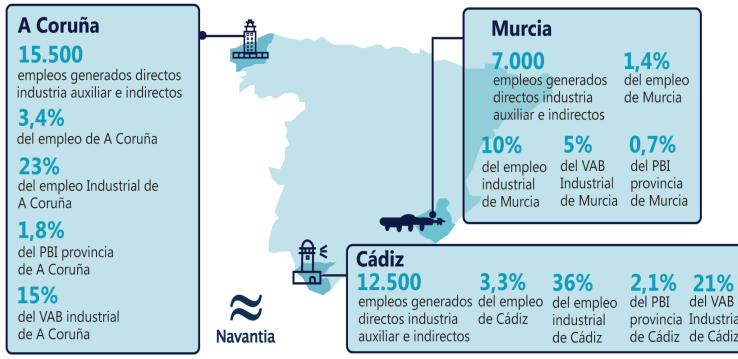


Figura 5: Astilleros e industria nacional.
Fuente: expuesto por el autor.

SESIÓN 3.2

C. de N.
Rudi
Quiñonez Benedetti

En toda actividad de las Fuerzas Armadas se distinguen procesos que permiten operar a sus integrantes, entre las cuales destaca la guerra electrónica. Estos procesos constituyen un flujo de información continua y permanente, basándose en tres acciones que complementan la toma de decisiones: reconocer, decidir y actuar.

En ese sentido, las Fuerzas Armadas continúan desarrollando y fortaleciendo sus capacidades en torno a la guerra electrónica. Asimismo, resulta fundamental, como primer paso de un sistema de gestión de combate, conocer la información determinada por el sistema de guerra electrónica, de modo que se convierta en un elemento esencial en sus esfuerzos por adoptar las competencias de comando, control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento.

En la actualidad, las industrias de defensa valoran la guerra electrónica, como una herramienta diseñada principalmente para usarse en contra de un adversario.

En este enfoque se enmarca la disertación de la ingeniera Cristina Von Beckh Widmanstetter, cuya especialización radica en el área de la electrónica, especialmente en el sector defensa. Por otro lado, cuenta con una amplia experiencia en el diseño de hardware y software de sistemas mage y contramedidas electrónicas ECM. Los temas que puntualizará en su presentación están ligados a las tecnologías emergentes para la defensa electrónica del buque y la identificación de la amenaza; a su vez, brindará una visión dedicada a las características y tecnologías clave para el sistema de defensa electrónica

de un buque, a partir de las exigencias que surgen en los escenarios, misiones actuales y las amenazas modernas que deben neutralizarse.

Ante esta situación, los escenarios y las misiones navales, que han cambiado en los últimos años, se traducen como un conjunto de desafíos que deben resolverse mediante los equipos de guerra electrónica, teniendo en cuenta que el espectro electromagnético es denso, diverso y dinámico.

Desde un enfoque industrial, estos nuevos desafíos abordarán las posibles soluciones desde un punto de vista funcional de los sistemas y equipos que conforman los sistemas de guerra electrónica, bajo un concepto de uso y respuesta ante un ataque cibernético.

Asimismo, el Dr. Félix Pérez Martínez, quien ha dedicado la mayor parte de su actividad profesional a la docencia e investigación en las áreas de las tecnologías de radiofrecuencia y los sistemas de radares, dirigirá su exposición hacia el futuro de los sistemas de guerra electrónica en el nuevo entorno del ciberespacio, teniendo en cuenta que, en los últimos años, la evolución de las características de los nuevos conflictos y la de los sistemas de información y comunicaciones devinieron en las Fuerzas Armadas de los países más avanzados. Naturalmente, esto afecta a los aspectos doctrinales, organizativos y operativos, en cuanto a la obtención del éxito en los nuevos conflictos ciber-electromagnéticos.

Este aspecto analiza el estado actual y la futura evolución de los sistemas de guerra electrónica, centrándose en cuestiones tecnológicas y técnicas, así como en las consecuencias de la aparición del ciberespacio como nuevo escenario de conflicto. Por otra parte, también atañe al proceso de convergencia entre la guerra electrónica y la ciberdefensa, y la previsible evolución de los sistemas de

este tipo de conflicto, como consecuencia de una visión funcional de la concurrencia entre la guerra electrónica, la ciberdefensa y la inteligencia electrónica.

Tal como menciona el doctor Pérez, la guerra electrónica ya no es un concepto que actúa de forma independiente, sino que está ligado a un gran sistema para ejercer actividades de mando y control, mientras que su importancia reside en la adquisición de la información en forma oportuna, eficiente y eficaz. Este aspecto es vital porque la superioridad de la información, obtenida mediante tecnologías de información y comunicación, se enmarca en el contexto operacional de los nuevos escenarios de conflictos que enfrenta en la actualidad, así como también en el protagonismo adquirido frente a esta nueva forma de guerra desarrollada en el ciberespacio, donde encontramos un estrecho vínculo entre la ciberdefensa y la guerra electrónica.

Al respecto, es posible obtener lo siguiente en base a estos dos enfoques: en el caso del primer tema, destaca una visión industrial, a corto plazo y más aplicada, que es lo que interesa a la empresa del sector defensa. Por otra parte, el segundo tópico se orienta hacia las soluciones a largo plazo, desde un punto de vista académico y conceptual. Cabe la posibilidad de que ambas exposiciones se traslapen, debido a que se encuentran orientadas a la evolución de los sistemas de guerra electrónica y al fortalecimiento de capacidades en cuanto a su uso en el ciberespacio.

En este punto, referido a la importancia de que los sistemas de defensa electrónica del buque y la identificación de la amenaza deben evolucionar para proporcionar una ventaja continua en la capacidad, mantenemos una interesante coincidencia y, en tal sentido, convenimos en que el sistema de alerta temprana del futuro debe ser capaz de operar en un entorno complejo, multidominio, multiorganizativo

y multinacional. Por lo tanto, los sistemas deben ser fácilmente modulares y escalables, proporcionando así una mejor cobertura y reduciendo la vulnerabilidad a los ataques electrónicos y físicos. En tal sentido, los sistemas tendrán que ser más selectivos, con el fin de ofrecer la identificación del emisor específico.

En cuanto a los sistemas del futuro, estos deberán obtener datos de otras fuentes como es el caso de los vehículos aéreos no tripulados, la adquisición de objetivos y el reconocimiento (istar). En este punto, el uso de los teléfonos inteligentes también requiere la capacidad de hacer frente a las aplicaciones de comunicación de voz y datos a través de redes celulares y wifi.

Por otra parte, la consciencia situacional es clave en cualquier dominio donde los efectos del uso de la tecnología y la creciente complejidad situacional afecten negativamente al ser humano en la toma decisiones. De tal manera, los futuros sistemas deben adaptarse al nuevo entorno ciberelectromagnético, mediante el desarrollo de nuevas arquitecturas y tecnologías. Es importante contar con un gestor GE que realice una interacción, en tiempo real, entre las informaciones obtenidas con los elementos activos, como resultado de la digitalización entre diversos sistemas de defensa que utilizan el espectro.

La Marina sabe que, como parte de la política, se desarrolló un sistema de guerra electrónica que, al conectarse a otros sistemas, brinda información al sistema de gestión de combate en la unidades tipo fragata misilera, la cual integra los sensores y el sistema de armas. Este desarrollo estará a la par con la tecnología emergente, que deberá adaptarse a la visión funcional de largo plazo para ser sostenible en el tiempo y obtenga la capacidad de adaptarse al estado de arte, manteniendo así la convergencia entre el ciberespacio y la inteligencia artificial.

sesión

3.2

Tecnologías emergentes para la defensa electrónica del buque y la identificación de la amenaza

Ing.
Cristina Von Beckh Widmanstetter

El objetivo de la guerra electrónica (GE, o EW por sus siglas en inglés) y sus tres componentes— EA (*Electronic Attack* o ataque electrónico), ES (*Electronic Support* o medidas de apoyo) y EP (*Electronic Protection* o protección electrónica, también llamada recientemente Electronic Defense en algunos contextos)— no es sólo resguardar una o más plataformas, sino también controlar, administrar y proteger el uso del espectro electromagnético (espectro EM, o EMS por sus siglas en inglés) con el objetivo de negárselo al enemigo.

Anteriormente, el interés de la GE por el espectro electromagnético en el ámbito naval se limitaba principalmente a los radares e históricamente a las comunicaciones. Hoy en día, el EMS contiene muchas otras señales, como las utilizadas para funciones fundamentales de posicionamiento y temporización, auxilios a la navegación y la auto-identificación de cada embarcación. Además, al estimarse que el 70% u 80% del tráfico mercantil actual se lleva a cabo por la vía marítima, es razonable suponer que estas nuevas señales y funciones aumentarán en el futuro.

En cuanto a las contramedidas, cabe destacar que las tecnologías situadas en las bandas del electróptico y microondas están iniciando una nueva época en cuanto a las armas de energía directa basadas sobre técnicas EMP (electro-magnetic pulse, high power, microwaves and Laser)

1. Escenarios navales

A continuación, haremos un repaso de los principales titulares periodísticos, que demuestran las distintas misiones y escenarios navales en los últimos tiempos:

ESCENARIOS y MISIONES

NATO blockade of Libya to close refugee route
EURACTIV.com with AFP
April 2016

OTAN bloquea Libia para cerrar la ruta de refugiados

Imagen 1.
Fuente: expuesto por el autor.

ESCENARIOS y MISIONES

Iran fury as Royal Marines seize tanker suspected of carrying oil to Syria ***The Guardian July 5, 2019***

Irán se enfurece cuando los Royal Marines se apoderan de un petrolero sospechoso de transportar petróleo a Siria

U.K. Says Iran Tried To Intercept Tanker In Strait Of Hormuz; Tehran Denies It
NPR World July 11, 2019

El Reino Unido declara que Irán intentó interceptar a un petrolero en el estrecho de Ormuz; Teherán lo niega

Imagen 2.
Fuente: expuesto por el autor.

ESCENARIOS y MISIONES

illegal, unreported and unregulated (IUU) fishing
pesca ilegal, no declarada y no reglamentada (INDNR)
worldoceanreview.com

Countries signed to UN-brokered illegal fishing treaty meet for first time ***UN News Centre May 2017***

Los países inscritos al tratado de pesca ilegal, negociado por la ONU, se reúnen por primera vez

Imagen 3.
Fuente: expuesto por el autor.

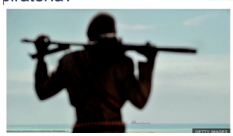
ESCENARIOS y MISIONES

Is Africa facing a new wave of piracy?
BBC May 2017

West Africa is becoming the world's piracy capital.
Piracy primarily affects three regions of the world: Africa, Southeast Asia, and Latin America

World Economic Forum Jun 2019

África se esta enfrentando a una nueva ola de piratería?



África occidental se está convirtiendo en la capital mundial de la piratería.

La piratería afecta principalmente a tres regiones del mundo: África, Sudeste Asiático y América Latina

Imagen 4.
Fuente: expuesto por el autor.

ESCENARIOS y MISIONES

Mass GPS Spoofing Attack in Black Sea?
galileognss.eu/ set 2017

Ataque masivo de suplantación de GPS en el Mar Negro

Imagen 5.
Fuente: expuesto por el autor.

ESCENARIOS y MISIONES

The Pakistan Navy detected an Indian submarine on Monday night trying to enter Pakistani waters ***CNN March 2019***

La Armada de Pakistán detectó un submarino indio el lunes por la noche tratando de entrar en aguas paquistaníes

Imagen 6.
Fuente: expuesto por el autor.

ESCENARIOS y MISIONES

Yemen's Houthis attack Saudi ship, launch ballistic missile
REUTERS JAN 2017

Los hutíes de Yemen atacan un barco saudí y lanzan misiles balísticos

Imagen 7.
Fuente: expuesto por el autor.

ESCENARIOS y MISIONES

USS Mason Fired 3 Missiles to Defend From Yemen Cruise Missiles Attack
USNI NEWS OCT 2016

El USS Mason disparó 3 misiles para defenderse del ataque de misiles por Yemer

Imagen 8.
Fuente: expuesto por el autor.

ESCENARIOS y MISIONES

The USS Cole sits off the coast of Yemen after a terrorist attack blew a hole in its side
CNN Oct 2000

El USS Cole frente a la costa de Yemen después de un ataque terrorista

What Insurgency Will Look Like in 2030
Defense One Apr 2019

Cómo será la insurgencia en 2030?

Imagen 9.
Fuente: expuesto por el autor.

Tras la revisión exhaustiva de estos hechos, queda comprobado que la industria naval militar debe responder a los desafíos actuales con un buque moderno multifuncional, flexible, ágil y capaz de operar en diferentes escenarios operativos, en solitario y en coordinación con otras unidades.

2. Desafíos

Los escenarios y misiones navales han cambiado mucho en los últimos años y se traducen en un conjunto de desafíos que deben ser resueltos por los equipos de GE, teniendo en cuenta que el espectro electromagnético es denso, diverso y dinámico. Además de los muchos emisores a bordo, debemos tener cuenta los siguientes puntos:

- Las emisiones *pop-up* y las llamadas fugitivas.
- La digitalización de las transmisiones.
- Las formas de onda de baja probabilidad de interceptación (LPI).
- Las nuevas emisiones de interés para la GE.
- Los escenarios litorales o de *brown waters*, así como la consecuente interferencia a alta potencia.

Por otro lado, también surgen nuevas amenazas como:

- Los ataques simultáneos y de distintas direcciones.
- Los sistemas de guía de amenazas multiespectro y la nueva generación de misiles balísticos.
- Los ataques cibernéticos.
- Los ataques asimétricos.

En tanto, otros aspectos que están condicionando los requisitos funcionales de un sistema de GE naval son:

Las tendencias en las operaciones militares:

- Las actividades red-céntricas.
- La colaboración entre sistemas tripulados y no-tripulados.
- La tendencia a reducir el número de miembros de la tripulación.

Las tendencias tecnológicas

La tecnología de uso civil/dual – Digitalización

En la actualidad, los avances tecnológicos están siendo guiados principalmente por la industria civil. Ejemplo de ello son los dispositivos electrónicos, la interconectividad y los equipos de entretenimiento, como los videojuegos. Estos avances, patentes en la elaboración de procesadores, enlaces, elementos estructurales de la red y transformación gráfica son tan importantes que los equipos militares no pueden más que beneficiarse de los mismos. Por otro lado, se reconoce la existencia de una mayor dependencia de estos, con todos los riesgos que ello conlleva, específicamente respecto al ataque cibernético.

Por otra parte, se está concretizando la concepción de tecnología de uso dual, la cual garantiza el uso de componentes elementales de estándar industrial (para condiciones de temperatura, vibración, entre otros) y la inclusión de funciones de protección y de resiliencia.

A nivel de trasmisión de señales, se está emigrando de esquemas de radiodifusión pura de una emisora potente, a los de transmisión celular. Este aspecto facilita el diseño de sensores y perturbadores en un esquema distribuido; la GE se puede intervenir en este proceso con un gran número de pequeños elementos idénticos de hardware, coordinados entre sí y realizando una parte de la tarea.

Por otro lado, la digitalización de las comunicaciones, la SDR *(software defined radio)* y el receptor digital han dado

flexibilidad a transmisiones difíciles de imaginar años atrás y que han poblado y ocupado el espectro EM de manera contundente.

3. Inteligencia artificial – redes neuronales

La inteligencia artificial y el uso de redes neuronales son tecnologías que están entrando en campos como la representación del conocimiento, el razonamiento y resolución de problemas, la planificación y el aprendizaje. En ese sentido, son elementos útiles en cuanto a la adaptación del comportamiento de un equipo de GE al dinamismo de un escenario EM, tanto en el punto de la presencia de emisores y amenazas, como a nivel de la señal y su comportamiento físico.

4. Requisitos funcionales

Los requisitos necesarios para responder a los desafíos de consciencia situacional son los siguientes:

- Poseer una arquitectura receptora que garantice la observación continua de todo el espectro EM de interés y que sea inmune a interferencias.
- Sensibilidad alta de receptor, siendo capaz de detectar señales de baja probabilidad de interceptación (LPI).
- Resolución alta de los parámetros medidos de la señal detectada.
- Blanking inteligente en tiempo y frecuencia.
- Contar con la capacidad de utilizar todas las emisiones de interés para crear una consciencia situacional óptima: identificación del emisor específico (o SEI por sus siglas en inglés).
- Capacidad de intercambiar información GE con otras plataformas.

Por el lado de los requisitos necesarios para responder a los desafíos de las contramedidas, están los siguientes:

– Capacidad de neutralización de distintas amenazas simultáneas y provenientes de distintas direcciones, lo que se denomina tecnología AESA (Active Electronic Scanning Antenna).

– Coordinación en tiempo real entre los sensores y perturbadores de GE y el sistema de combate.

– Velocidad y capacidad de detección y neutralización de amenazas desde las primeras fases del proceso de ataque.

– Velocidad y capacidad de detección y neutralización de amenazas desde las primeras fases del proceso de ataque.

– Monitoreo constante de la situación EM, para anticipar la presencia y/o neutralizar la amenaza asimétrica.

5. Tecnologías

Las funciones esenciales de la GE se basan sobre las siguientes tecnologías:

– Digitalización.

– Avances tecnológicos de los componentes de microondas.

– Los convertidores analógico-digitales de frecuencia de muestreo cada vez mayor.

– Amplificadores de banda ancha.

– Los enlaces híper veloces.

– Conmutadores híper veloces.

– Componentes programables y ASIC (ambos de altísima velocidad y capacidad de transformación de datos).

6. Consciencia Situacional

La posibilidad de procesar las señales del espectro EM en

tiempo y en frecuencia ha creado un sinfín de posibilidades de análisis numérico, las cuales observaremos a continuación:

Arquitectura MAGE (Medidas de Apoyo a la Guerra Electrónica)

Los requisitos de un sistema MAGE se pueden definir sinteticamente como:

- Ambiente denso.
- Alta sensibilidad.
- 100% POI.
- DF de alta precisión.

Una arquitectura MAGE ideal debe mantener la capacidad de observación de todo el espectro EM de interés, interceptando las emisoras fugitivas y las señales de baja probabilidad de detección. Hoy en día, esto se obtiene mediante un doble camino de observación y análisis del espectro, contenidos en un único receptor MAGE. En tanto, los elementos fundamentales son:

- **Función de recepción digital a banda ultra ancha UWB DRx**

  Es la capacidad mediante la cual el espectro se mantiene vigilado constantemente y protegido, gracias a la posibilidad de cancelación dinámica de interferencias.

- **Función de recepción digital banda ancha canalizada múltiple WB DRx**

  Escanea una porción del espectro a la vez, aplicando transformaciones a la señal en frecuencia y en otros dominios, detectando todas las señales de interés.

Los avances en las tecnologías de componentes de muestreo y transformación de señal están permitiendo el desarrollo de nuevas arquitecturas llamadas *direct sampling* (o muestreo

directo), las cuales evitan el uso de componentes analógicos como los convertidores descendientes. Estas arquitecturas no mejoran significativamente las características de actuación, pero permitirán una disminución de costos y la obtención de un equipo GE de dimensión, peso y requisitos de alimentación mucho menores, lo cual es importante para las plataformas aéreas.

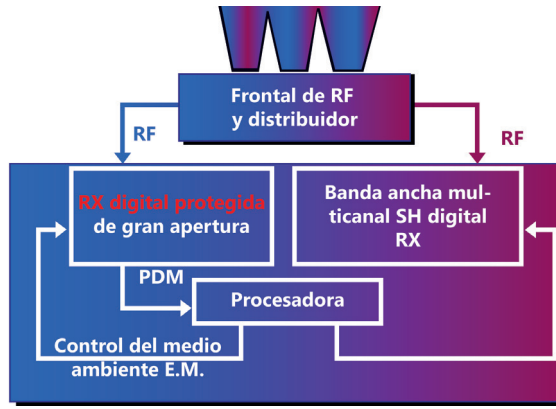


Figura I: el espectro EM.
Fuente: expuesto por el autor.

7. Detección de Señales LPI

Estas señales tienen una potencia instantánea muy por debajo del ruido de un receptor MAGE tradicional y distribuyen la energía en el tiempo con una duración significativa del pulso. Con los actuales algoritmos de transformación de señal es posible recuperar decenas de decibeles que permiten la detección y análisis de estas señales en tiempo real.

8. Transformación SEI

La transformación SEI (identificación del emisor específico) se basa en un análisis de la señal en tiempo, frecuencia y otros dominios. De forma similar al análisis ELINT de un radar, pero en tiempo real, la transformación SEI permite identificar

específicamente a un emisor y distinguirlo de otros del mismo modelo de producción, ubicando inequívocamente la plataforma donde esté embarcado. Esta capacidad da lugar a numerosas aplicaciones con cualquier tipo de señal en contextos de aguas azules, litorales y escenarios híbridos, particularmente con barcos que no quieren ser reconocidos y no realizan transmisiones, incluso si transmitiesen datos AIS falsos. Por otra parte, las pruebas efectuadas en campo real arrojaron valores de reconocimiento con fiabilidad del 85% y 95%, después de diez impulsos. En tal forma, las señales de aplicación son variadas y entre ellas se cuentan a los radares de navegación y las señales AIS.

9. Contramedidas

Los requisitos de un sistema de contramedidas electrónicas se pueden definir sintéticamente como:

- Técnicas sofisticadas de perturbación.
- Número de amenazas neutralizadas dentro de la cobertura espacial total.
- Alto ERP – alta potencia irradiada efectiva, alta sensibilidad.
- Fuerte integración entre RESM y RECM para una reacción rápida.
- Manejo de interferencias.

10. Memoria digital de radiofrecuencias DRFM

Las técnicas sofisticadas de perturbación se obtienen mediante la DRFM (*Digital radiofrequency memory*) que es un objeto digitaliza y memoriza la señal de radar enemigo, para sucesivamente aplicar sobre ésta los algoritmos de modulación de señal e implementar la técnica de contramedida deseada y que será transmitida. El concepto del DRFM existe desde los años 80 y, hoy en día, ha mejorado la fiabilidad, referida a una mayor resolución de parámetros con la cual logra engañar el radar enemigo; esto

debe contrarrestar la capacidad del radar en cuanto a la distinción de una señal eco, mediante los mismos avances tecnológicos que apoyan al ECCM.

11. AESA

La tecnología AESA, también llamada uso de antenas de matriz activa escaneada electrónicamente, con dirección de haz electrónico en planos de acimut / elevación, para una cobertura instantánea de acimut de 360°, es la que resuelve el ataque simultáneo de varias amenazas provenientes de distintas direcciones.

La alta eficiencia y generación de energía, basada en la tecnología de matriz en estado sólido, permiten implementar una solución compacta de transmisores dentro de un volumen reducido. Estas características dan paso a formas de onda y técnicas de interferencia inteligentes y efectivas que mejoran los rendimientos de interferencia y la protección del barco, logrando una potencia radiada efectiva muy alta (ERP) con un ciclo de trabajo total, eficiente y fiable.

Por otro lado, el sistema de contramedidas AESA precisa módulos de trasmisión y recepción para garantizar una velocidad y calidad de respuesta óptima. La reacción a tiempo compartido se logra a través de un esquema adaptativo basado en un número de rastreadores PRI (cada uno asignado a una amenaza) que operan en paralelo y en una lógica selectora basada en la prioridad de amenaza.

El uso de módulos transmisión/recepción a estado sólido (en el pasado conformado por GaAs y ahora en GaN) permite integrar algunas funciones de recepción al MAGE embarcado, utilizando altísimas ganancias de antena y resolución de dirección de llegada de una matriz de antenas. Cabe mencionar que los equipos de contramedidas de tecnología AESA, con módulos de transmisión/recepción, son operativos en varios buques de las marinas militares europeas.

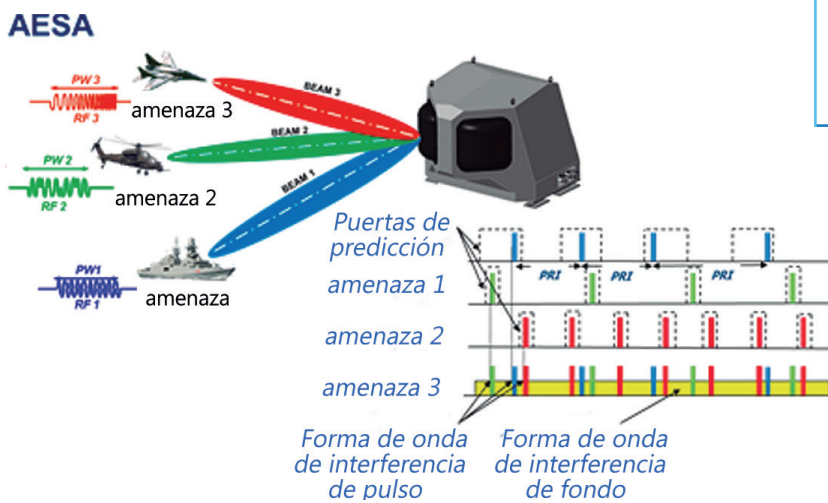


Figura 2: equipos de contramedidas de tecnología AESA con módulos de transmisión/recepción.
Fuente: expuesto por el autor.

12. Concepto de uso

Recordemos algunas declaraciones fundamentales de G.E. suscritas entre Europa y la OTAN:

- La guerra electrónica es un multiplicador de fuerza *(EW is a force multiplier).*
- El control del espectro electromagnético es un objetivo esencial y crítico *(Control of the EM spectrum (EMS) is an essential and critical objective).*
- La guerra electrónica está orientada hacia las tareas o la misión *(Electronic warfare is task oriented).*

Estamos de acuerdo con las primeras dos declaraciones. La tercera declaración, sin embargo, nos recuerda que hay que evitar lo siguiente:

- La evaluación de un equipo GE en base a las mejores tecnologías disponibles, cuando quizás no todas sean necesarias.

– La excelente actuación de un equipo de GE se desaprovecha debido a un concepto de uso no adecuado (por ejemplo, los datos llegan demasiado tarde al destinatario).

– La formación exigua.

En otras palabras, la tecnología sola no es suficiente.

13. Gestor de GE (EW Manager)

Un gestor del GE (o EWM por sus siglas en inglés) es necesario para todas las plataformas aéreas, navales y terrestres. Sus funciones principales son:

– Supervisar y gestionar el funcionamiento general de todos los subsistemas y la conexión con los demás componentes del sistema de combate.

– Elaborar el escenario táctico del entorno electromagnético, utilizando sensores a nivel de plataforma (sensores RESM, CESM, E / O, entre otros).

– Presentar el resultado sintético de las interceptaciones, según el formato establecido para operaciones red-céntricas.

– Coordinar, en algunos casos, con los sensores de GE de otras plataformas embarcadas (helicóptero, UAV) para obtener una consciencia situacional extensa.

– Definir e implementar las acciones de participación de GE contra emisiones del escenario táctico indicadas como amenazas, utilizando perturbadores de GE como los subsistemas RECM, DLS, entre otros.

En un buque, el gestor EWM y su colaboración con el sistema de combate son esenciales, ya que optimizan el tiempo de respuesta a un ataque en las primeras fases de búsqueda y adquisición del radar enemigo, como en

la coordinación con los demás equipos del sistema de combate.

Una interfaz hombre-máquina eficiente es la prueba de un buen gestor de GE y de un óptimo concepto de su uso. En tanto, el sistema de contramedidas propone al sistema de combate distintas modalidades de reacción, con diferentes niveles de automatismo, lo que proporcionará al operador del GE toda la información táctica necesaria en tiempo real, como el índice de eficiencia de la contramedida aplicada. Cabe precisar que el sistema de combate del buque mantiene siempre el control absoluto sobre el equipo de GE.

14. Respuesta al Ataque Cibernético

Al igual que cualquier plataforma, un buque es vulnerable frente a los ataques cibernéticos. Identificar los puntos de entrada y los vectores de un ataque son acciones fundamentales y precisan un análisis detallado. Sin embargo, los principales segmentos de dicho análisis serían:

- **Personal (voluntaria e involuntariamente)**

  A pesar de las muchas campañas de sensibilización, el personal sigue siendo el principal método de acceso de un ataque cibernético. En tal sentido, el uso no controlado de dispositivos electrónicos personales representa uno de los mayores vectores de un ataque.

- **Los equipos hardware y software**

  Ya sean de proveedores comerciales o militares. Los proveedores de equipos como Elettronica, por ejemplo,respetan las regulaciones y estándares de diseño (common criteria EAL) que incluye encriptación, firewall, accesos controlados y monitoreo, uso de componentes trusted y componentes de gestión de tránsito de datos a alta resiliencia.

- **Enlaces de comunicación alámbricos e inalámbricos**

  En el segundo aspecto, encontraremos la superposición con la GE tradicional. Ejemplos reales en el ámbito naval incluyen ataques a los sistemas de navegación tipo GPS y los ataques a trasmisiones satelitales.

En un buque se implementarán todas las medidas necesarias para mejorar la resiliencia en estos tres segmentos, pero se reconoce que obtener un 100 % de inmunidad es imposible.

Por este motivo, el enfoque actual en el mundo militar es la recuperación de la capacidad militar durante un ataque cibernético, aunque sea de forma parcial. Dicha recuperación no es banal y requiere una serie de pasos como la detección del ataque, identificación del daño y las funciones comprometidas a nivel de sistema de combate, aislamiento o neutralización del daño, la renuncia a ciertas funciones y el accionar de funciones alternativas, con el fin de proseguir la misión.

Definir los procesos de recuperación/reactivación en un buque es una tarea difícil y crítica. Por ello, la tripulación debe ser continuamente formada. En pocas palabras, la resiliencia al ataque cibernético se obtiene con:

- Seguridad por diseño.
- Identificación y clasificación automatizada de amenazas.
- Prácticas de respuesta a medida.
- Capacidades SOAR *(Security Orchestration Analysis and Response).*

15.- Formación

La tecnología de los videojuegos y la realidad virtual ofrece productos de interfaz hombre-máquina de altísimo nivel de realismo. Gracias a los circuitos de gestión de imágenes,

los operadores pueden realizar sesiones de formación de GE excelentes sin necesidad de subirse a bordo de una plataforma real. Asimismo, los simuladores de sistemas GE respetan la dinámica de las plataformas, las características de las amenazas y la actuación del equipo embarcado. Cabe mencionar lo interesantes que son los laboratorios dw simulación de GE combinados, en los que los distintos operadores (operador MAGE, piloto de helicóptero, piloto de avión no tripulado) realizan una misión conjunta.

16. Conclusiones

Las altísimas actuaciones de conmutadores a radiofrecuencia, frecuencia de muestreo, bandas instantáneas de los convertidores analógico digitales, sintonía de receptores superheterodina, escansión electrónica de arreglo de antenas, junto con velocidades y capacidad de componentes de transformación digital, son tecnologías disponibles en la actualidad que permiten una gestión del espectro electromagnético comparable con la duración del mismo impulso radar.

- Éstas son concebidas bajo criterios funcionales para resolver los desafíos de los equipos de GE de una unidad de superficie, con el objetivo de crear una conciencia situacional eficaz y una defensa del buque contra amenazas simultáneas múltiples.
- En el futuro inmediato, la inteligencia artificial, el muestreo analógico digital directo a radiofrecuencia, sensores y actuadores distribuidos, las armas de energía directa, entre otros, jugarán papeles importantes en el desarrollo de los equipos de GE de nueva generación.

sesión

3.2

Los futuros sistemas de guerra electrónica en el nuevo entorno del ciberespacio

Dr.
Félix
Pérez Martínez

El objeto de esta ponencia es analizar el estado actual y la futura evolución de los sistemas de guerra electrónica, centrándonos fundamentalmente en los aspectos tecnológicos y técnicos, así como en las consecuencias de la aparición del ciberespacio como nuevo escenario de conflicto.

1. Introducción

Hasta hace unos años, la ciberdefensa y la guerra electrónica han sido conceptos bastante alejados entre sí, tanto doctrinal como operativamente. En muchas fuerzas armadas, como las de Estados Unidos de América, la inteligencia electrónica externa al combate no es considerada como parte de la guerra electrónica, pues se le asocia exclusivamente al uso y control táctico del espectro electromagnético, durante el transcurso de los combates.

Por otro lado, el ciberespacio ha sido asociado siempre a los sistemas de información constituidos por redes de ordenadores convencionales (redes de área local) con gran capacidad de computación, que se conectaban entre sí mediante enlaces dedicados y seguros; en cuanto a las amenazas, estas se introducían por puertas externas e internas asociadas a las vulnerabilidades del software. La ciberdefensa se desarrollaba fundamentalmente en este contexto, siendo muy influenciada por una ciberseguridad en constante y rápido desarrollo en el ámbito civil. Esto se dio a pesar de que una de las definiciones de ciberespacio, enunciado en los primeros años de este siglo, en base a la Estrategia Militar Nacional para Operaciones del Ciberespacio, lo describe como un dominio caracterizado por el uso de la electrónica y el espectro electromagnético, para almacenar, modificar e intercambiar datos a través de la red y los sistemas e infraestructuras físicas asociadas.

En los últimos años, la evolución de las características de los conflictos y los sistemas de información y comunicaciones

imposibilitan mantener estos ámbitos alejados, por lo que han iniciado transformaciones muy significativas en las fuerzas armadas de los países más avanzados, afectando aspectos doctrinales, organizativos y operativos, para tener éxito en los nuevos conflictos ciberelectromagnéticos en los que se combinan y convergen acciones de ambos ámbitos (ver figura 1). En ese sentido, es muy probable que el conflicto del Donbáss, ocurrido al este de Ucrania e iniciado el año 2014, suponga un punto de inflexión en esta convergencia, la cual era evidente unos años antes.

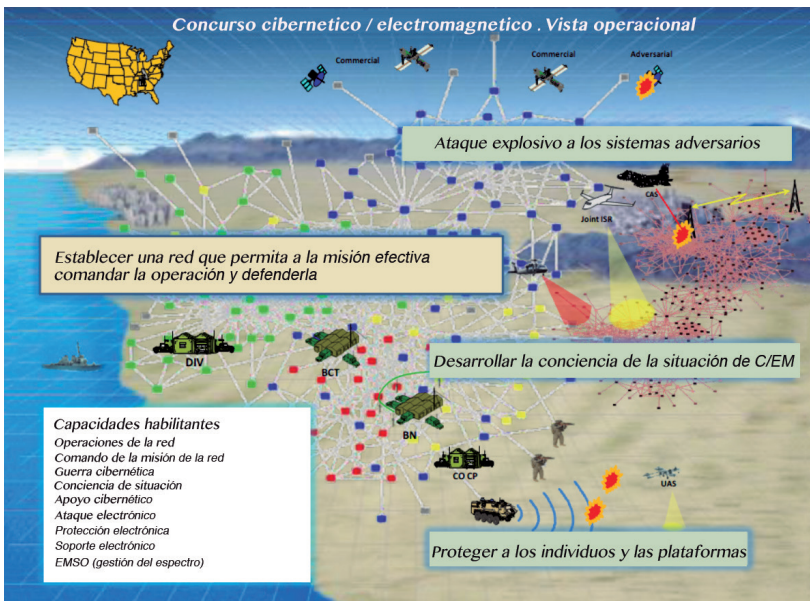


Figura 1: acciones ciberelectromagnéticas (vista operativa)[1].
Fuente: expuesto por el autor.

En tanto, la guerra electrónica es definida como el conjunto de acciones militares orientadas a determinar, explotar, reducir o prevenir el uso hostil del espectro electromagnético por el enemigo, así como a mantener su utilización por parte de las fuerzas propias. Su objetivo es

el control de espectro electromagnético, lo cual se obtiene de la siguiente manera[2] (ver figura 2):

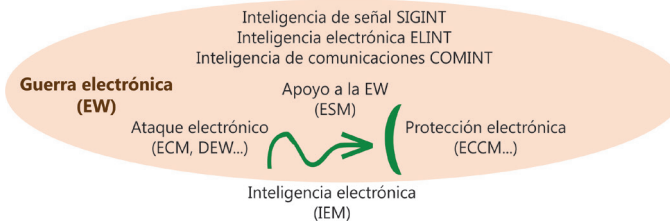


Figura 2: actividades de Guerra Electrónica.
Fuente: expuesto por el autor.

Medidas de apoyo a la Guerra Electrónica (ESM)

Son acciones adoptadas con el objetivo de buscar, interceptar, identificar y/o ubicar a cualquier equipo o dispositivo que utilice el espectro electromagnético, para obtener[2] el reconocimiento inmediato de la amenaza. Las operaciones de ESM se pueden clasificar en SIGINT, ELINT y COMINT (inteligencia de señales, electrónica y de comunicaciones).

Ataque electrónico

Es un conjunto de acciones orientadas al uso de energías electromagnéticas para atacar a personas, infraestructuras y equipos. La misión de estos actos es degradar, neutralizar y destruir la capacidad de combate del enemigo. Asimismo, incluye, entre otras actividades, las contramedidas electrónicas (ECM o también llamadas *Electronic Countermeasures*) y las armas de energía dirigida (*DEW o Directed Energy Weapons*).

Medidas de protección electrónica (EPM)

Son acciones tomadas para proteger a las personas, infraestructuras y equipos, de los efectos producidos por fuerzas propias o enemigas de las acciones de EW que degraden, neutralicen o destruyan la capacidad de combate

propia. Se suele llamarlas anti-contramedidas electrónicas (*ECCM o Electronic-Counter-Countermeasures*) e incluyen, entre otras actividades, la introducción de subsistemas específicos en oposición a las ECM, el control de emisiones, el empleo de comunicaciones seguras, la reducción de firmas y el apantallamiento y protección electromagnética de los equipos.

Como se ha indicado, la **inteligencia electrónica no táctica** (en tiempo de paz) es considerada, en muchas fuerzas armadas, separada orgánicamente de la guerra electrónica, hecho que es cada día más difícil de mantener, en opinión del autor de este texto. La guerra electrónica se ha desarrollado exponencialmente desde la Segunda Guerra Mundial, hasta convertirse en un elemento imprescindible en los actuales escenarios de conflicto, especialmente durante la segunda mitad del siglo pasado. Es un ejemplo de actividad sometida a la dinámica proyectil-blindaje, donde los sucesivos desarrollos de uno de los elementos no hacen sino fomentar el desarrollo del otro. En otras cuestiones, podríamos decir que es un mecanismo de realimentación traducido en una complejidad creciente de los sistemas electrónicos empleados en aplicaciones de defensa, seguridad y en el uso masivo del espectro electromagnético.

La guerra electrónica, a nivel tecnológico y operativo, se desarrolló en el entorno de la Guerra Fría y su evolución respondió a las necesidades de este tipo de conflicto. No es extraño que, tras la caída del Muro de Berlín, esta entrase en crisis, limitando su desarrollo fundamentalmente a los sistemas de autoprotección de plataformas y personas. Esta situación afectó especialmente a los ejércitos de tierra, que disponen de pocas plataformas con el nivel de sofisticación y coste de buques y aviones. Simultáneamente, el incremento exponencial del uso de sistemas de información y de sus vulnerabilidades, propició que la mayor parte de los recursos se dedicasen

a sistemas y unidades de ciberseguridad e inteligencia electrónica estratégica, en detrimento de los tradicionales sistemas y unidades de guerra electrónica. En palabras de MAJ Michael Senft[3]:

> *"The Army maintained communications electronic warfare battalions during the Cold War, but were disbanded in the 1990s, causing significant deficiencies in electronic warfare capabilities, which were grimly recognized during combat operations in Iraq and Afghanistan. With less than 1,000 officers, warrant officers and enlisted personnel, the EW career field has struggled with finding its role as combat deployments have significantly decreased".*

Esta situación parece no haber cambiado, si se piensa en algunos comentarios sobre los conflictos de Ucrania y Siria.

Sin embargo, no ocurrió lo mismo en Rusia, cuyo interés por la guerra electrónica se ha mantenido a lo largo del tiempo, tal como se deduce de una cita del general Raymond Thomas, en la cual señala que :

> *"Right now in Syria we are operating in the most aggressive EW environment on the planet from our adversaries. They are testing us everyday, knocking our communications down, disabling our EC-130s ..." (Thomas, 2018)*

Tal como se indica en la referencia, el Estado Mayor General de Rusia considera la EW como una respuesta asimétrica a la superioridad tecnológica de la OTAN. En la figura 3 se presentan algunos de los últimos desarrollos rusos en guerra electrónica, que en su doctrina incluye las acciones de ciberdefensa. Las figuras han sido obtenidas de la referencia[5], en la que se describe muy bien la situación actual.

SISTEMA EN FUNCIÓN	
RB - 341 Leer-3	Interferencia de las comunicaciones
RB - 301B Borisoglebsk-2	Sistema automático de interferencia (detección, búsqueda de dirección, análisis y supresión de radiocomunicaciones HF/VHF). Incluye puesto de mando R-330KMV y varias estaciones
R- 934UM	Sistema automático de radio (detección, búsqueda de dirección, análisis y supresión de radiocomunicaciones HF/VHF). Incluye puesto de mando R-330M1P y los sistemas automáticos de interferencia Diabazol
R- 330Zh Zhitel	Sistema automático SATCOM/GPS/GSM (detección, búsqueda de dirección, análisis y supresión de radiocomunicaciones UHF). Parte de R-330M1P y los sistemas automáticos de interferencia Diabazol
Shipovnik - Aero	Sistema de intercepción UAV
Torn	Sistema automático de radio (especificaciones desconocidas; actualmente no están en servicio)
Rtut-BM	La proximidad de la radio fue la estación de interferencia (protegiendo al personal y al equipo de las municiones)
RB - 636AM2 Svet-KU	Monitorea las ondas de radio y rastrea varias fuentes emisoras de radio
R-318T Taran	Sistema de comunicación. Incluye el puesto de mando y varias estaciones que operan en el rango HF/VHF/UHF
MKTK-1A Djudist	Sistema de control de radio y protección de la información (detección, direccionamiento y análisis de las señales de radio) destinado a ayudar al control de las emisiones

Se informa que el sistema de interferencia de radar Rusia Krasukha - 2 se ha desplegado en Siria

Borisoglebsk- Sistema de alerta temprana de largo alcance

Figura 3: ejemplos de equipos rusos de guerra electrónica de última generación[4]. Fuente: expuesto por el autor.

Por otro lado, los conflictos han evolucionado hacia una gran complejidad, producto de múltiples factores como la globalización, los cambios demográficos y de entorno, la descomposición de algunos estados, la propagación de ideologías y movimientos radicales, la aparición de nuevos entornos de conflicto (como el ciberespacio) la escasez de algunos recursos, entre otros. Además de los conflictos convencionales, han surgido nuevos tipos como los asimétricos —de creciente sofisticación a medida que se facilita y abarata el acceso a las tecnologías emergentes— y los híbridos, donde los enfrentamientos se libran simultáneamente en el ámbito militar y civil.

En definitiva, las operaciones militares se han transformado, pasando de poner énfasis en las características cuantitativas de la guerra (masa y volumen) en los que la potencia del armamento y la capacidad de ocupar el terreno eran garantía de éxito, a otro tipo de operaciones más sofisticadas, en las que se debe lograr ventaja física, temporal o condicional sobre adversarios de muy diversa naturaleza.

Cabe mencionar que algunos conflictos se libran como batallas de la información, en los que los sistemas de información y telecomunicaciones juegan un papel esencial y, sobre ellos, se desarrollan las acciones de guerra electrónica y ciberdefensa. De hecho, en este nuevo entorno, el despliegue y operación de infraestructuras de información y comunicaciones juega un papel esencial en cuanto a la integración de sensores, redes de comunicaciones y sistemas de información. Esto dotará a las unidades combatientes de la precisa superioridad de la información.

Figura 4: visión funcional de la convergencia entre la guerra electrónica, la ciberdefensa y la inteligencia electrónica.
Fuente: expuesto por el autor.

2. La convergencia entre la guerra electrónica y la ciberdefensa

En la figura 4 se presenta una vista funcional de las relaciones y fronteras entre las operaciones de guerra electrónica (óvalo marrón), inteligencia electrónica (óvalo azul) y ciberdefensa (óvalo rojo). Esta es una modificación realizada por el autor de un gráfico presentado en la referencia[6]. Se trata de una figura relativamente antigua que demuestra que, en términos teóricos, es difícil separar las actividades en los tres ámbitos.

Conviene destacar que, aunque en el siglo pasado estaba enunciada la posibilidad de utilizar efectos combinados entre los tres tipos de operaciones, estas eran ejecutadas por diferentes unidades militares, por lo que parece más una aproximación teórica que una realidad. Sin embargo, desde hace una decena de años, se está produciendo una clara convergencia entre las actividades de guerra electrónica y la ciberdefensa en un contexto caracterizado por la aparición de los combates híbridos (en el que convergen sistemas militares y civiles. El de Ucrania es un ejemplo claro de este tipo de conflicto) y la creciente importancia del uso militar de técnicas y tecnologías civiles en muy rápido desarrollo.

En el año 2012, en un artículo muy interesante[7], Rohret y Jimenez pusieron de manifiesto la integración de protocolos IP en los sistemas que utilizan radio frecuencia (RF). Esto permite atacar redes aisladas con mucha facilidad, pues su protección cibernética frente a las acciones de Guerra electrónica se centran en las vulnerabilidades dentro de sus respectivas áreas y no en los efectos combinados. La amenaza se ve acentuada por las vulnerabilidades introducidas durante la integración de hardware y software. En el artículo de presentan tres casos de estudio en los que se evalúan vulnerabilidades reales de tres sistemas:

- Un sistema de IP sobre radio desarrollado para proporcionar comunicaciones de banda ancha entre una plataforma aérea y de tierra, que se interrumpió sin que se atribuyese el hecho a un ataque (detectado como un error del sistema).
- Una red de comunicación por satélite que, tras ser perturbada, pasó a utilizar canales mucho más vulnerables.
- Una red de sensores que se degradó hasta cortar los datos, sin que se activase ninguna alarma.

Otro caso muy conocido en el ámbito civil es la perturbación de sistemas de comunicaciones móviles 3G y 4G, para que conmuten a sistemas 2G mucho más vulnerables. Algo similar puede hacerse con las redes de WiFi, al buscar el uso de las que posean mayor vulnerabilidad. En definitiva, y frente a los ataques clásicos de las guerra electrónica, los efectos combinados dificultan la detección e identificación de la fuente del ataque.

Un hecho muy significativo que conviene resaltar es que, si bien el incremento exponencial de las capacidades de proceso y almacenamiento de información propiciada por los avances de la microelectrónica, conocida como la Ley de Moore, es la base de la actual revolución digital, no es menos cierto que, en los últimos años, solo se

ha podido satisfacer los requisitos de computación con nuevas arquitecturas en los sistemas de información y comunicaciones, en los que la computación de la información se hace en la nube (*cloud computing*) en el borde y en la niebla (*edge and fog computing*); mediante ellas se consiguió un espectacular crecimiento de la mencionada capacidad de computación y almacenamiento por la reducción de costes de infraestructura, flexibilidad en su disponibilidad y escalado, y rapidez de despliegue. Todo ello era inimaginable hace sólo unos años y ha sido posible gracias al desarrollo, también exponencial, de las técnicas y tecnologías de conectividad.

En efecto, esta distribución espacial y temporal del proceso de computación (ver un ejemplo en la figura 5) supone el futuro de los sistemas hiperconectados, en los que las comunicaciones basadas en el uso del espectro electromagnético juegan un papel esencial e implica que

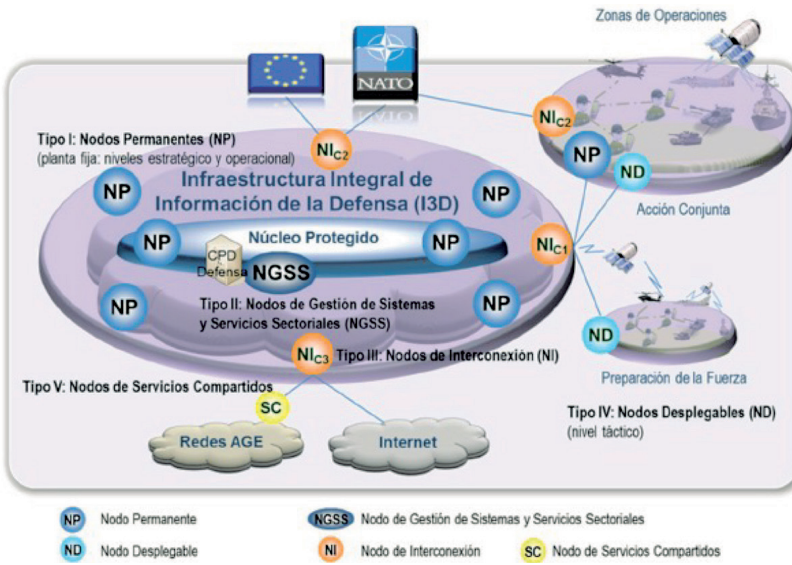


Figura 5: estructura y tipos de nodos CIS/TIC del Ministerio de Defensa de España[8].
Fuente: expuesto por el autor.

una buena parte de las vulnerabilidades de los sistemas queden en el aire. Por otro lado, la llegada del internet de las cosas (IoT) o el próximo despliegue del 5G acelerará el mencionado proceso en el campo civil y se trasladará, tarde o temprano, al ámbito militar. En este nuevo escenario, la convergencia de la guerra electrónica y la ciberdefensa es inevitable en lo que ya se denominan actividades ciberelectromagnéticas.

En definitiva, las técnicas de guerra electrónica y ciberdefensa se modificarán drásticamente en los próximos años, pues la convergencia de las mismas es necesaria para mantener la eficacia de las operaciones. Desde hace algunos años, se están creando unidades conjuntas, especialmente en los países en los que la transformación digital de las actividades de la Defensa está más avanzada. A modo de ejemplo, consúltese la referencia[9], en la que se presenta un caso de integración en una división de guerra cibernética y electrónica, la cual integra capacidades tecnológicas para cubrir las necesidades del ciberespacio y el entorno electromagnético. Por otra parte, en estas referencias encontrarán propuestas de integración doctrinal y operativa[10 11].

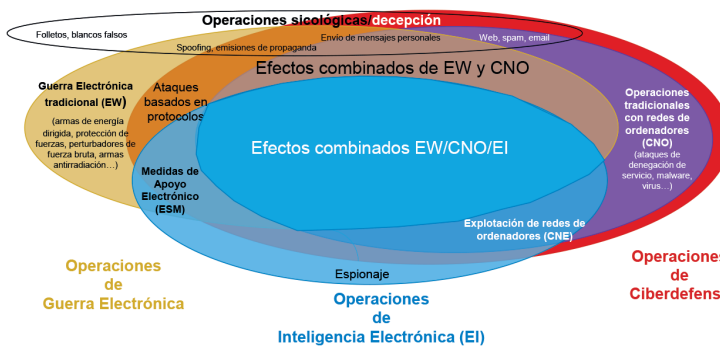


Figura 6: visión funcional de la convergencia futura de la guerra electrónica, la ciberdefensa y la inteligencia electrónica. Fuente: expuesto por el autor.

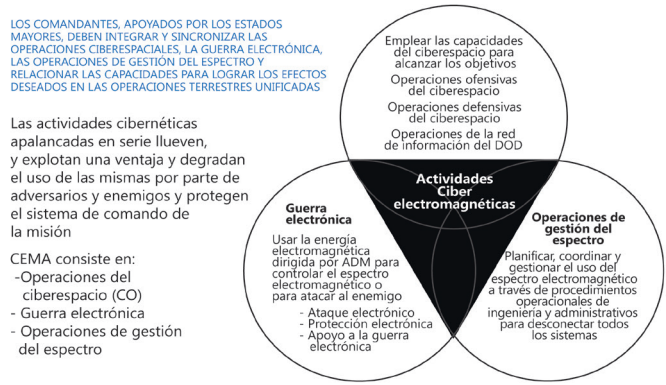


Figura 7: actividades ciberelectromagnéticas.
Fuente: expuesto por el autor.

3. Los futuros sistemas de Guerra Electrónica

Organización, doctrina y operaciones

Desde el punto de vista organizativo y operacional, la evolución principal de los actuales sistemas de guerra electrónica está representada por la figura 7, la cual fue tomada de la referencia 1.

En tal forma, la nueva visión CEMA (*Cyber and electromagnetic activities*) pretende la sincronización y coordinación de las actividades en ambos ámbitos y en estos momentos se considera algo esencial para el éxito de las futuras operaciones militares[12].

Su implementación implica importantes cambios estructurales, doctrinales y operativos en las Fuerzas Armadas, las mismas que no son objeto de este documento, pero que constituyen un reto tan importante o más que la transformación tecnológica que se comentará a continuación[13] [14].

Nuevos retos técnicos

Los principales retos a los que deberán enfrentarse los sistemas de guerra electrónica en los próximos años, los

mismos que condicionarán los posteriores desarrollos de los equipos y los sistemas son los siguientes:

- La adaptación de los mismos al nuevo entorno ciberelectromagnético.
- La necesidad de combatir la amenaza más importante en los próximos años para las plataformas, una amenaza todavía no resuelta, nos referimos a las nuevas generaciones de misiles supersónicos.

Ambas retos, especialmente en el caso de las Fuerzas Armadas más avanzadas tecnológicamente, significarán una excelente oportunidad para la industria de Defensa de sus países, en cuanto al desarrollo de nuevas arquitecturas y tecnologías capaces de no sólo abordar estos retos, sino también de responder a las necesidades de los futuros escenarios de conflicto en los que la densidad del espectro electromagnético será enorme.

Arquitecturas

Se están haciendo importantes esfuerzos por implementar arquitecturas que permitan la generación de sistemas adaptativos y reutilizables, buscando tanto su aplicabilidad en entornos cambiantes y la multifuncionalidad con vistas a la reducción drástica de costes. Ambos objetivos se conseguirán digitalizando, lo antes posible, la cadena del proceso y con anchuras de banda de las señales digitalizadas.

Se presentan los componentes básicos de un sistema convencional de guerra electrónica. La principal característica de las arquitecturas empleadas es la separación funcional entre los sensores y los perturbadores en casi todos los casos, con una participación humana muy importante en la toma de decisiones relativa a la selección de los perturbadores, a partir de las amenazas

detectadas por los sensores (sólo en algunos sistemas específicos de autoprotección, sensores y perturbadores trabajan de modo automático recogiendo las señales y retransmitiéndolas con alguna modificación en sus parámetros) tal comolo observamos bien, en la figura 8.

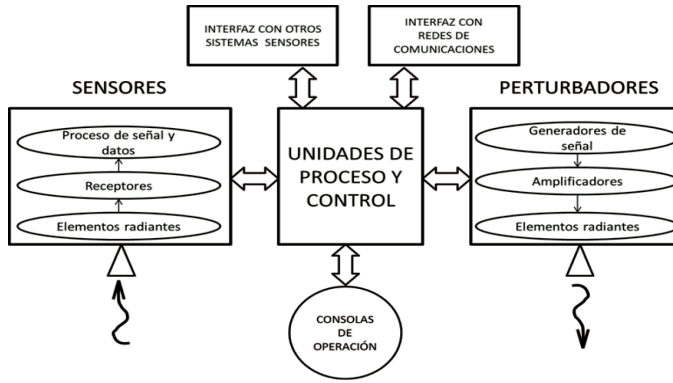


Figura 8: elementos de un sistema de guerra electrónica.
Fuente: expuesto por el autor.

Asimismo, tanto los sensores como los perturbadores están bastante especializados en determinadas amenazas definidas previamente por las acciones de inteligencia electrónica.

Por el contrario, las tendencias básicas en las nuevas arquitecturas se caracterizan por permitir una interacción en tiempo real entre las informaciones obtenidas por los sensores y las señales enviadas al entorno por los perturbadores, estableciendo sistemas cognitivos en los que la intervención humana será más de control que de ejecución. Los elementos claves para conseguirlo se presentan en los esquemas de la figura 9 [15] [16].

Nótese que en el esquema de la página de la derecha que no sólo son utilizables los módulos para distintas aplicaciones, sino que mediante la misma antena es posible transmitir y recibir.

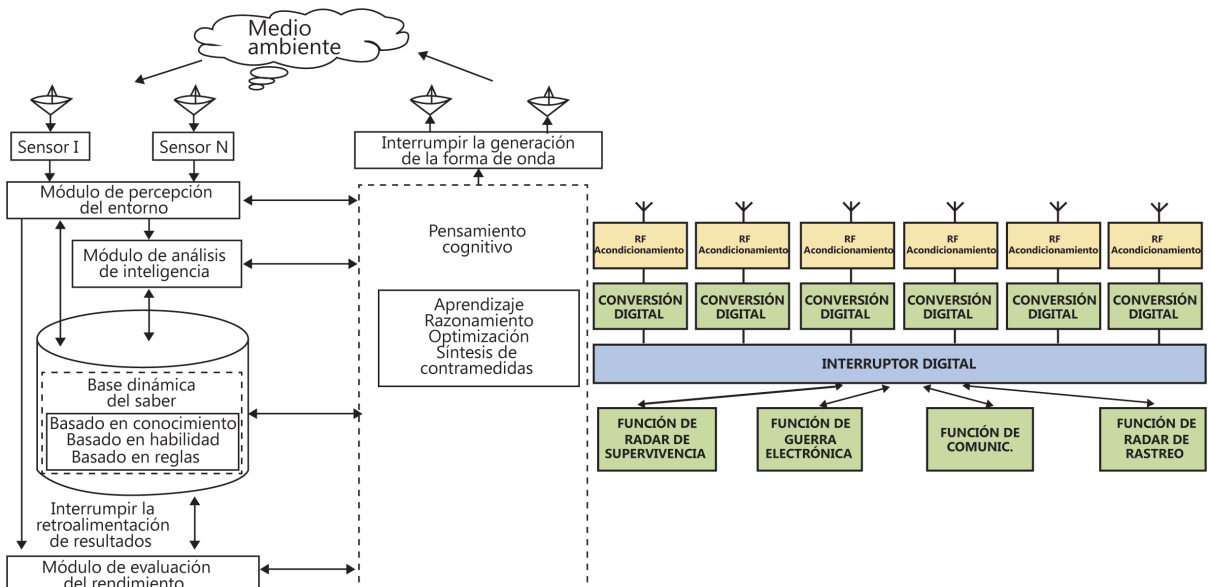


Figura 9: tendencias para las nuevas arquitecturas de sistema de guerra electrónica.
Fuente: expuesto por el autor.

Tecnologías

Las tecnologías clave que soportarán todo lo expuesto en los párrafos anteriores empiezan por el desarrollo de arquitecturas AESA (*Active Electronically Scanned Array*) de bandas ultra-ancha, las cuales permitirán la discriminación espacial, tanto en recepción como en transmisión y de forma ágil.

A su vez, permitirán la combinación espacial de potencia y la capacidad de trabajar con varios blancos simultáneos. Por otro lado, se desarrollarán antenas y componentes de RF/MW, milimétricas y de varias octavas de ancho de banda capaces de

a. recepcionar, detectar, discriminar, identificar y seguir instantáneamente señales en bandas ultra-anchas (receptores FSSR o Full-Spectrum Staring Receiver) para combatir las técnicas de frequency hopping y, en general, las técnicas LPI (Low Probability of interception) su realización requiere el desarrollo de técnicas de digitalización a muy alta velocidad

b. emisión y generación de señales de alta dinámica –en potencia y tiempo- en las mismas bandas (transmisión).

Para ello, se requieren sofisticadas técnicas de miniaturización de componentes de alta frecuencia, como los empleados en el *transceptor de Mercuy Systems Mercury's* RFM3101[17], capaces de trabajar entre 6 y 18 GHz con anchos de banda instantáneos de 1GHz. La vigilancia/perturbación de toda la banda requiere 12 transceptores, pero en los próximos años, tras el incremento de las velocidades de conversores y procesadores, serán posibles canalizaciones más eficientes.

– Es preciso tomar en cuenta también el *desarrollo de nuevos componentes, circuitos y subsistemas de estado sólido, en particular los basados en nitruro de galio (GaN*) para realizar nuevos transmisores

de estado sólido, de alta eficiencia, alto margen dinámico y subsistemas miniaturizados. Con estos componentes se desarrollará la nueva generación de perturbadores, llamados también jammers, para sustituir a los TWT (Traveling Wave Tube Amplifiers) y permitir el manejo de señales adecuadas a la guerra cibernética.

– En otro campo, está la *aplicación de las técnicas SDR (Software define radio)* la cual refiere la flexibilidad y adaptabilidad suministrada por estas técnicas en los nuevos sistemas de comunicaciones; esto obliga a introducirlas tanto en los receptores como en los transmisores de guerra electrónica y será una tecnología clave en la extensión de las actividades de ataque ciberelectromagnético.

– Aplicando *técnicas de SDR (software Define Radio)*. a los sistemas de guerra electrónica, es posible implementarlas en plataformas pequeñas y de bajo coste, con tasas de muestreo de GHz y procesamiento basado en FPGA, que son capacidades operativas sofisticadas que manejan altas velocidades de datos.

– También tenemos las *armas de energía dirigida*, el desarrollo de los láseres de alta potencia, así como los espejos y lentes que, si bien soportan estas energías, hecho comprobado en los laboratorios, en el campo de batalla no surtieron efectos significativos. Asimismo, su uso en las bandas de RF/MW y milimétricas, para atacar sistemas de navegación y telemetría, de comunicaciones y redes de sensores será muy importante en los próximos años, especialmente cuando estas armas se embarquen en las UAS.

– En el caso de los *sistemas de integración de las UAS (Unmanned Aircraft Systems)*, se tiene como una alternativa distribuida a los actuales sistemas de vigilancia, autoprotección y ataques basados en grandes plataformas terrestres, marítimas o aéreas. Obviamente las potencias requeridas por los perturbadores son muy inferiores en cuanto a la posibilidad de perder los UAS.

– La conformación de *sistemas de vigilancia basados en arrays* de antenas, cuyos elementos estén situados en las UAS, es una posibilidad teórica con grandes dificultades prácticas de carácter tecnológico, operativo y de costes.

– Finalmente, la *introducción masiva de técnicas de inteligencia artificial* refiere a una de las tecnologías más disruptivas en los próximos diez años, debido al incremento radical de la potencia computacional, la disponibilidad de grandes cantidades de datos y los avances sin precedentes en redes neuronales profundas; esto permitirá que los sistemas de ciberguerra aprovechen los datos para adaptarse a las situaciones cambiantes del combate.

Por otro lado, es el camino a un escenario más complejo, en el que combatirán sistemas de guerra electrónica autónomos y UAEWS (Unmanned and Autonomous EW Systems).

4. A modo de conclusión

En los párrafos anteriores se ha realizado un ejercicio de especulación sobre la posible evolución de los actuales sistemas de guerra electrónica, como consecuencia de tres tendencias de convergencia entre ámbitos que, hasta

hace unas décadas, estaban muy separados. De ello, se concluye lo siguiente:

- La ciberdefensa y la guerra electrónica convergen en los nuevos conflictos ciberelectromagnéticos.
- La convergencia tecnológica es fruto de la digitalización entre los diversos sistemas de defensa que utilizan el medio radioeléctrico para conseguir sus objetivos, mediante las aplicaciones de seguridad y defensa, y las tecnologías desarrolladas en los sectores civiles y militares.

Todo ello augura una transformación muy importante de los actuales sistemas de guerra electrónica en los próximos años.

Notas

1) Ackermann, T. (2018). Electronic Warfare Trump's Cyber for Deterring Russia. Recuperado de https://breakingdefense.com/2018/02/electronic-warfare-trumps-cyber-for-deterring-russia/

2) Anónimo. Recuperado de https://www.dst.defence.gov.au/research-division/cyber-and-electronic-warfare-division

3) Cyber Electromagnetic Activities FM 3-38. (2019). Recuperado de https://publicintelligence.net/us-army-cema/

4) Cohen, S. (2018) Integrating Cyber and Electronic Warfare. Signal. March 5, 2018. Recuperado de https://www.afcea.org/content/integrating-cyber-and-electronic-warfare

5) De Martino, C. (2019) Wideband Microwave Transceiver Strives for Versatility. Microwave & RF. Recuperado de https://www.mwrf.com/systems/wideband-microwave-transceiver-strives-versatility

6) Headquarters, Department of the Army. (2017). Cyberspace and Electronic Warfare Operations FM 3-12. Recuperado de https://fas.org/irp/doddir/army/fm3-12.pdf

7) Manrique Montojo, F. (2019). Panorama de la guerra electrónica en Rusia. Documento de Opinión IEEE 11/2019. Instituto Español de Estudios Estratégicos. Madrid, España. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO11_2019FERMAN-ejercitoRusia.pdf

8) Martínez, F. *Documentación del Máster en Sistemas de Comunicación e Información para la Defensa y la Seguridad (4ª ed.) Módulos: Sistemas ESM*, ECM y EPM sobre sistemas de comunicaciones, ECM y EPM sobre sistemas sensores. Universidad Politécnica de Madrid.

9) Microwave Journal (2019) Electronic Warfare Market Redefining the Strength of the Defense Industry". Recuperado de https://www.microwavejournal.com/articles/32536-electronic-warfare-market-redefining-the-strength-of-the-defense-industry

10) Ministerio de Defensa de España (2017). Arquitectura Global de Sistemas y Tecnologías de Información Y Comunicaciones del Ministerio de Defensa (AG CIS/TIC). Recuperado de https://publicaciones.defensa.gob.es/arquitectura-global-de-sistemas-y-tecnologias-de-informacion-y-comunicaciones-del-ministerio-de-defensa-ag-cis-tic.html

11) Porche, I. et al (2013). Redefining Information Warfare Boundaries for an Army in a Wireless Word. United States Army. RAND Corporation monograph series. Recuperado de https://www.rand.org/pubs/monographs/MG1113.html

12) Rohret, D. & Jimenez, A. (2012). *Convergence of Electronic Warfare and Computer Network Exploitation/Attacks Within the Radio Frequency Spectrum*. Proceedings of ICIW 2012, The 7th International Conference on Information-Warfare & Security.(consultado el 9 de Agosto de 2019)

13) Senft, M. (2016). Convergence of Cyberspace Operations and Electronic Warfare Effects. The Cyber Defense Review. January 04, 2016. Recuperado de https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136055/convergence-of-cyberspace-operations-and-electronic-warfare-effects/

14) Trimmer, B (2011). Trend in Defence Electronics: Thecnological Convergence in Radar and EW. Microwave Journal September 2011. Recuperado de https://www.microwavejournal.com/articles/11683-trends-in-defence-electronics-technological-convergence-in-radar-and-ew

15) UK Ministry of Defence Crown (2018). Cyber and Electromagnetic Activities . Joint Doctrine Note (JDN) 1/18. The Development, Concepts and Doctrine Centre (DCDC). Recuperado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf (consultado el 9 de Agosto de 2019)

16) Watson, D. (1998). *Diseño Práctico de Buques*. Elsevier Science ltd. Reino Unido: Oxford.

17) Xiao, Q (2018). A Conceptual Architecture of Cognitive Electronic Warfare System. The Tenth International Conference on Advance Cognitive Technologies and Applications. Recuperado de http://www.thinkmind.org/index.php?view=article&articleid=cognitive_2018_3_10_40012

Carlos Spolita
William Bundy
José Ángel Gallego
Eduardo González

INNOVACIÓN TECNOLÓGICA

BLOQUE 4

BLOQUE

4

MODERADORES

EXPOSITORES

SESIÓN 4.1

C.de N.
Renato
Antonioli Ríos

En primer lugar, quiero agradecer al señor Carlos Spolita, encargado de simulación de la empresa Warsila/ Transas, por la exposición que nos brindará, respecto a cómo viene impactando la tecnología en la operación de los sistemas marítimos.

El impacto de la tecnología en estos sistemas ofrece diversos retos y desafíos, tanto en el presente como en el futuro, principalmente en las estructuras vinculadas a las labores de maniobra y navegación, así como también en el uso de simuladores. Esto permite la mejora continua en el entrenamiento y a muy bajo costo.

Al respecto, quiero comentarles que en la Marina de Guerra del Perú ha iniciado el proceso de implementación de simuladores de maniobra y navegación en la Escuela Naval, lo que redundará en provecho de los cadetes navales; asimismo, nos encontramos en un proceso de modernización a través del sistema offset y del simulador táctico-operacional, para la toma de decisiones de los comandos de las unidades operativas de la institución.

Acto seguido, el doctor Eduardo Gonzales, de la Escuela de Ingeniería y Ciencias del Tecnológico de Monterrey – México, nos presentará como la evolución de la tecnología conlleva a la optimización de los resultados educativos. Por otro lado, veremos también como el sistema AVATAR contribuye a esta mejora, a gran distancia y de manera interactiva.

sesión

4.1

El impacto de la tecnología en los procesos de educación y operación de los sistemas marítimos

Lic.
Carlos Spolita

Durante muchos años, el arte de la navegación ha mantenido características y procedimientos tradicionales para la resolución de problemas propios e inherentes, como la determinación de la posición del buque, el cálculo de su rumbo y velocidad, entre otras. En ese sentido, teniendo presente su carácter tradicional, aún hoy se encuentran a bordo elementos como el sextante, el compás magnético, las alidadas y reglas paralelas. Estos materiales siguen siendo necesarios para hacerse a la mar, de manera segura y eficiente, en base a los métodos de navegación tradicional.

Asimismo, la operación marítima ha incorporado herramientas que vienen transformando lentamente todos esos procesos, junto con el método de trabajo y aprendizaje a bordo de los buques. Una de las soluciones más transformadoras y emblemáticas fue la inclusión de los sistemas ECDIS (Sistema de Información y Visualización de Cartas Electrónicas) como herramienta primaria de navegación, en reemplazo de la cartografía náutica en papel.

En cuanto a la importancia de este equipo y el cambio que originó a partir del año 2012, se incluye la obligatoriedad, de manera gradual, en la implementación y utilización de esta herramienta en los buques regidos bajo el convenio SOLAS (Convenio Internacional para la Seguridad de la Vida Humana en el Mar). En la actualidad, nos encontramos con buques que poseen un sistema dual ECDIS y que ya no utilizan la cartografía náutica clásica en sus operaciones.

A través del ECDIS, refiriéndome específicamente al sistema **Wärtsilä Navi Sailor 4000**, el personal navegante realiza una cantidad importante de tareas digitales propias del seguimiento de la navegación y la seguridad náutica. Entre ellas podemos destacar el chequeo de posición, la utilización de la cartografía náutica electrónica (CNE) y su actualización, la verificación de alarmas para evitar varaduras y colisiones, generación y seguimientos de

rutas, seguimientos de blancos AIS y radar, obtención de distancias y profundidades, así como también el proceso de integración con sensores. Esto demuestra la forma en que se han modificado los comportamientos y procesos operacionales, en base a la digitalización de tareas que históricamente se efectuaban de forma manual.

Ahora bien, para lograr una correcta aplicación de todas estas nuevas capacidades y herramientas tecnológicas, se debe recurrir al entrenamiento a través de un ***simulador***. Mediante este método, se obtendrá la familiarización con los sistemas y el uso óptimo de los mismos, dando como resultado una navegación **segura y eficiente**.

A través del Código STCW (*International Convention on Standards of Training and Watchkeeping for Seafarers*), que configura las enmiendas de Manila 2010, se refleja la prioridad y obligatoriedad de entrenar a los hombres de mar mediante el uso de simuladores; con la simulación se busca mejorar sus competencias, evaluar sus conocimientos, desempeños y habilidades, para prevenir accidentes marinos y disminuir los riesgos de contaminación ambiental. A través de sus distintas plataformas, Wärtsilä provee las soluciones de entrenamiento requeridas y establecidas por la regulación internacional actual, para los simuladores de navegación **Wärtsilä Navi Trainer Professional 5000**, simuladores de comunicaciones o GMDSS **Wärtsilä TGS 5000** y los simuladores técnicos para el área de máquinas, cargas líquidas y grúas **Wärtsilä TECH SIM 5000**.

En efecto, **Wärtsilä** es una empresa líder a nivel mundial, debido a que ofrece soluciones de avanzada para el mercado marítimo (mercante y naval). Uno de sus objetivos es maximizar el rendimiento económico y medioambiental de los buques y equipos a bordo de sus clientes, poniendo énfasis en la innovación tecnológica y la eficiencia total. Además, busca contribuir en el avance de sociedades sustentables a través del desarrollo de soluciones de tecnología **inteligente**.

En mayo de 2018, el grupo tecnológico **Wärtsilä** adquirió la empresa **Transas**, con el objetivo de acelerar el camino de Wärtsilä hacia la configuración de una visión estratégica denominada ***Ecosistema Marino Inteligente (Smart Marine Ecosystem)***.

Fundada en 1990, Transas es una empresa que lidera el mercado de soluciones de tecnología marítima, incluyendo desde sistemas de navegación ECDIS y ECS, sistemas de navegación para buques militares (WECDIS), puentes de navegación integrados, productos y servicios digitales de cartografía náutica electrónica privada (TX 97) y en formato oficial S-57, hasta sistemas de control de tráfico marítimo, control de puertos (VTS) y sistemas de vigilancia costera , monitoreo de buques y una gama de soluciones de simulación requeridas para el entrenamiento respectivo en el uso de los sistemas anteriores.

Por otro lado, también están incluidas la certificación del personal de abordo y la ejecución de estudios de I+D, que son procesos propios del ámbito marítimo, portuario y naval. Con más de 5500 simuladores instalados, 300 sistemas de tráfico marítimo operando en puertos del mundo y más de trece mil sistemas de navegación en uso, Wärtsilä se ha convertido en líder mundial del sector y en una compañía ampliamente reconocida por su trayectoria, calidad y grado de innovación.

Los objetivos de Wärtsilä están dirigidos a transformar la industria en un **ecosistema marino inteligente**, así como a la mejora de la eficiencia de las operaciones en toda la cadena de valor, la neutralización del impacto climático y la optimización de la seguridad para la industria del transporte marítimo, dirigiendo operaciones sustentables, seguras y rentables para el sector marítimo, en particular para las compañías navieras y operadores globales. De esta manera, se busca desarrollar herramientas de tecnología inteligentes que hagan realidad la estrategia del SME, al conectar los puertos inteligentes con los

buques que operan en el espacio marítimo global y que han sido entrenados con sistemas de simulación de última generación.

En este sentido, siguiendo dicha estrategia, una de las soluciones lanzadas por Wärtsilä es la denominada ***Fleet Operation Solution (FOS)***. Esta solución, cuya estructura está basada en una plataforma única, como **sistema de gestión de flota**, integra desde el buque su sistema de navegación (ECDIS) y una estación de planificación ***(Navi Planner)*** las cuales, a través de la nube y en un ambiente seguro, permiten el acceso de herramientas para el análisis de datos, optimización y aprendizaje automático. Por otro lado, facilitan el mantenimiento y entrenamiento para la gestión de buques de una flota determinada, mediante aplicaciones móviles abordo y/o en tierra. Este sistema está diseñado para conseguir el más alto nivel

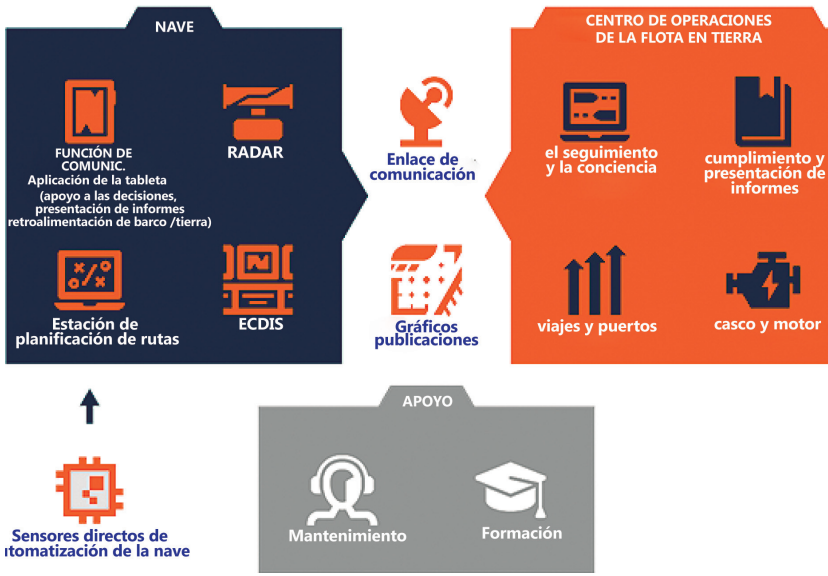


Figura I: arquitectura Fleet Operation Solutions – FOS.
Fuente: expuesto por el autor.

de seguridad en el mar, aumentar la eficiencia de la flota y simplificar las tareas diarias tanto en tierra como a bordo.

Como podemos observar, las operaciones marítimas están siendo digitalizadas a una velocidad incalculable, lo que hace prever que esta tendencia seguirá incrementándose debido al mayor y fácil acceso a las comunicaciones existentes y la tecnología disponible. Esta tendencia se encuentra apoyada por los organismos internacionales, en los cuales se gestan nuevas regulaciones basadas en exigencias ambientales y de seguridad, puntos motivados y dinamizados por la tecnología disponible y existente.

Por otra parte, las nuevas soluciones que forman parte de la visión de un ecosistema apuntan a mejorar las operaciones, haciéndolas más eficientes y seguras, pero requieren un entrenamiento adecuado para lograr un uso óptimo de ellas. Por ello, los simuladores siempre tendrán un rol primario para su implementación efectiva; precisamente, Wärtsilä se encuentra a la vanguardia y trabajando en este sentido, verificando que los productos de simulación puedan cubrir las necesidades y desafíos que plantean las operaciones marítimas en la actualidad.

Esta tendencia nos invita a evaluar internamente si nuestras organizaciones se encuentran preparadas para los nuevos desafíos y si los sistemas de entrenamiento son capaces de cubrir las necesidades actuales y futuras que imponen las nuevas tendencias y soluciones tecnológicas. Tengamos en cuenta que los hombres de mar estamos expuestos a este fenómeno, en todos los ámbitos de actividad.

sesión

4.1

Tecnología educativa

Dr.
Eduardo
González Mendivil

La evolución de las herramientas tecnológicas ha permitido aumentar la calidad de la telepresencia en el aula. En tanto, la experiencia de uso de un robot con proyección holográfica se reporta en clases oficiales de nivel universitario impartidas en el TEC de Monterrey, durante el año 2013 hasta el 2016. Esta combinación permite a los estudiantes "sentir" la presencia del profesor en el aula, a través de una imagen holográfica a escala humana, audio bidireccional, video y movimientos autónomos de un robot controlado a distancia. En cuanto a los reportes del uso individual y combinado de estos dispositivos de telepresencia, los resultados señalan que estamos en el camino correcto.

Este trabajo ha tenido eco en la comunidad latinoamericana, principalmente en Uruguay, Colombia, Argentina y Chile. Asimismo, se muestra como una forma de propagación de esta información y como invitación a que otros investigadores en el mundo colaboren acumulando experiencia, formalidad y rigor científico en torno a ella.

1. Introducción

La tecnología de videotelefonía tuvo su primer gran avance en 1964. Hace 50 años, la empresa AT&T presentó por primera vez el servicio de teleimagen en la Feria de Nueva York; sorprendentemente, la invención del videoteléfono no tuvo el éxito esperado y se concluyó que los costos elevados, la mala calidad y la falta de voluntad del consumidor para interactuar con las cámaras detuvieron su desarrollo. Este hecho fue reconocido como el primer evento documentado de la telepresencia.

De este modo, pasó un cuarto de siglo hasta que, a principios de la década de 1980, la red digital hizo posible la compresión existente entre video y audio de larga distancia. Desde entonces, la videotelefonía evidencia un crecimiento sostenible en la rama personal y empresarial. Precisamente, en estas aristas encontramos insertado el

campo de la educación a distancia, la cual ha pasado por tres etapas de desarrollo.

La primera es conocida como la fase impresa, en la cual nuestros antepasados contrataban servicios educativos y estos les llegaban por correo. Una vez cubierto todo el material, remitían una evaluación escrita para recibir un diploma y el acceso al siguiente nivel. Por otra parte, la segunda etapa fue denominada como analógica e incluyó el uso de la televisión abierta y por cable, así como el envío de videos y programas de radio. Finalmente, la tercera etapa, llamada también fase digital, se caracterizó por el uso del internet (Luévano Belmonte, López de Lara y Edward Castro, 2015).

Los avances más recientes, como las aplicaciones de mensajes de texto, estimularon aún más la eficiencia en la comunicación en el trabajo. Hemos recorrido un largo camino desde los días de las cartas y memorandos escritos, incluso el correo electrónico se ha convertido en una forma secundaria de comunicación en el trabajo, a medida que las plataformas de chat se utilizan cada vez más. Aquí es donde entra el concepto de "telepresencia", el cual consiste en una combinación de tecnologías que buscan representar a una persona ubicada en un lugar distante, como si estuviese físicamente en un recinto determinado.

2. ¿Qué es la telepresencia?

Hace más de 30 años, Marvin Minsky, profesor del MIT y pionero en los estudios acerca de la inteligencia artificial, presentó un ambicioso plan para el desarrollo de sistemas robóticos teleoperados avanzados, que marcarían el comienzo de una economía a control remoto. Asimismo, en 1980, escribió sobre esto en la revista de ciencia ficción Omni; en su ensayo, el Dr. Minsky imaginó una economía controlada a distancia y acuñó el término "telepresencia" para describir estos sistemas que, en su visión futurista,

transformarían el trabajo, la fabricación, la producción de energía, la medicina y muchos otras facetas de la vida moderna (Minsky, 2010).

2.1. ¿Qué es la telepresencia holográfica?

Es un sistema que proyecta imágenes de movimiento completo, realistas y 3D en tiempo real. Un sistema de telepresencia holográfica captura sonidos e imágenes de personas reales, remotas y objetos circundantes, comprimiéndolas y transmitiéndolas a través de una red de banda ancha. Una vez transmitidas, las imágenes son descomprimidas y proyectadas, incluyendo además la comunicación de audio en tiempo real, lo cual mejora aún más el realismo de la experiencia. En algunos casos, podría competir realmente con la presencia física de un usuario, en otras palabras, la telepresencia constituye la combinación de una o más tecnologías, con la proyección holográfica como el principal medio de comunicación entre los usuarios.

En ese sentido, tenemos al Profesor Avatar, que es un modelo de telepresencia desarrollado en el Tecnológico de Monterrey, el cual combina el uso de proyecciones holográficas en tiempo real y robots de telepresencia. Por otra parte, ofrece la oportunidad de impartir educación en lugares donde las circunstancias geográficas, la inseguridad o el costo imposibilitan el acceso a este servicio, mediante especialistas tele presentes, tutores y parejas de estudiantes que interactúan en tiempo real intercambiando conocimientos y experiencias de diversos contextos.

En ese sentido, el maestro o especialista puede ver y escuchar a los estudiantes en tiempo real, ofreciendo atención especial y una retroalimentación inmediata. Este modelo ofrece la experiencia contar con un profesor en el aula, pero en forma holográfica, proporcionando movilidad virtual desde cualquier parte del mundo e interacción

personalizada con los estudiantes. Al ver al profesor a escala humana se genera una suma de emociones entre los estudiantes, ya que perciben que el profesor está realmente en el salón de clases. Esto representa la humanización de la educación a larga distancia.

Este proyecto ha sido aceptado en comunidades educativas y empresariales, debido a la gran expectativa generada con respecto a su potencial de desarrollo y escalabilidad. Por ello, colegas profesionales de todo el mundo, inmersos en entornos educativos y empresariales, han mostrado interés por replicar esta propuesta, ya que para ellos representa una solución a varios problemas que enfrentan en su vida diaria, como los costos elevados de transporte, inseguridad, movilidad, dispersión geográfica de los establecimientos y atención remota personalizada y en tiempo real. A su vez, permite importantes ahorros de costos y proporciona movilidad a un número limitado de tutores y estudiantes. Esta iniciativa constituye un medio de transmisión de ideas, conocimientos y experiencias de líderes, empresarios y guías de pensadores en el proceso de enseñanza-aprendizaje. Por otro lado, este modelo es flexible porque se adapta a diferentes metodologías y estilos de aprendizaje (Luévano Belmonte, Telepresence technologies to humanize distance education, 2017).

El principal beneficio de este proyecto consiste en ofrecer soluciones innovadoras, de bajo costo, fácilmente escalables y adaptables a diferentes estilos de aprendizaje, específicamente en el campo educativo. El hecho de conectarse a través de robots de telepresencia y/o proyecciones holográficas en tiempo real ofrece la oportunidad de generar un canal de comunicación avanzado, donde cualquier maestro, independientemente del nivel académico o materia que enseñe, podrá brindar atención personalizada a sus alumnos como si estuviesen presentes físicamente. Esto produce una genuina sensación de acompañamiento entre los estudiantes (durante el

proceso de aprendizaje-enseñanza) a diferencia de las videoconferencias tradicionales en las que el profesor presuntamente está ausente.

3. Experiencia previa

Cuando un grupo de investigadores, conformado por profesores del campus central de la Universidad Tecnológica de Monterrey, incursionó en actividades que requerían de proyecciones holográficas, se produjo una colaboración efectiva con maestros ubicados en el campus de Zacatecas, quienes adquirieron posteriormente una estación holográfica.

Esta proyección en vivo, con robots de telepresencia incluidos, es el resultado de una larga historia de experiencia, observación y aprendizaje, desarrollado a lo largo de nueve años por el profesor Eduardo Luévano, colaborador en la Universidad Virtual del TEC de Monterrey, después de 15 años de experiencia como profesor de Contabilidad y Finanzas, y facilitador en materias impartidas en el modelo virtual. En base a este proceso, el profesor Luévano concluyó que es difícil retener la atención del grupo porque, de cierta manera, la pantalla es un objeto estático que puede ignorarse fácilmente. En ese sentido, el profesor no tiene acceso visual a toda el aula y resulta fácil evadirlo; por otro lado, no es posible dar comentarios en tiempo real sobre el desempeño personal de cada uno de los estudiantes. En el modelo virtual real, las clases con alto contenido cuantitativo no permiten que el profesor preste la atención adecuada al progreso del alumno durante la sesión (Luévano, López de Lara y Castro, 2015).

4. Telepresencia, proyección holográfica y robot

El profesor Luévano realizó diversos trabajos para conseguir que el proceso de la educación a larga distancia sea más eficiente, por lo que dirigió sus investigaciones hacia el concepto de telepresencia. En base a esa experiencia, propusimos el uso de un robot de telepresencia denominado

"Profesor Avatar", cuyo objetivo era el de reducir las limitaciones actuales del modelo de videoconferencia conocido. Este experimento tuvo lugar en el campus de Zacatecas del TEC de Monterrey, desde septiembre del 2012 hasta mayo del 2013.

Buscando mejorar la sensación de telepresencia dada por el profesor, propusimos integrar la proyección holográfica como complemento adicional a la educación a distancia. Creemos que, al integrar las tecnologías existentes como la videoconferencia, el robot de telepresencia y la proyección de hologramas, podremos ensamblar un paquete tecnológico que permitirá suplir (pero nunca reemplazar) la ausencia física y temporal del maestro en el aula. En tal sentido, suficientes elementos predicen los beneficios del uso intenso de la tecnología de telepresencia.

Ahora, describiremos la experiencia que tuvimos al usar una combinación de recursos tecnológicos. Adquirimos una lámina de proyección holográfica transparente al 90% para construir la pantalla; esta lámina se adhirió a un vidrio de 12 mm, anclado a una base metálica estable y soportada sobre ruedas para facilitar su movimiento. Esta pantalla permite visualizar imágenes tridimensionales sin distorsión. Cabe mencionarles que este es un producto importado, cuya presentación es en rollo y con diferentes longitudes, en un ancho estándar de 1,52 m. El costo de este material es de 3250 pesos mexicanos por metro lineal. De este modo, construimos dos pantallas con una altura de 1,80 m, tal como consta en la figura 1 (Luévano Belmonte, López de Lara y Edward Castro, Use of Telepresence and Holographic Projection Mobile Device for College Degree Level, 2015).

Al hacer la proyección en la pantalla transparente, la lámina retiene los fotones proyectados; luego, la imagen del profesor aparece como si estuviera flotando, configurando el resultado final de la telepresencia: la persona está allí, sin embargo, no está. Es importante notar la transparencia,

Figura I: clase de Telepresencia Holográfica del Campus Tec de Monterrey en Zacatecas.
Fuente: expuesto por el autor.

ya que es posible observar los muebles y la pantalla blanca detrás del soporte transparente, hecho que ofrece una sensación muy real. Con la intención de mejorar la percepción de telepresencia entre los estudiantes, integramos la pantalla holográfica, el robot y el software para controlar la proyección a larga distancia.

5. El I-Challenge

La telepresencia, a través de la proyección holográfica, se ha utilizado en los últimos años en la impartición de conferencias internacionales. Sin embargo, en cuanto a la realización de estas actividades a nivel universitario, solo se cuenta con un registro de iniciativas experimentales. La telepresencia, junto con la proyección holográfica aplicada en un curso de universidad, permitirá al profesor dar su clase a tiempo y en forma novedosa cuando él no esté dentro del aula, desestimando las restricciones en cuanto a distancia, clima o diferencia horaria.

Esta tecnología permite ahorrar costos porque no será necesario viajar a otras ciudades para dar una clase, conferencia o reunión. Sin embargo, el uso de la proyección holográfica no es meramente académico, ya que puede ser versátil y multipropósito en las universidades, (Luévano y

López de Lara, Uso de Dispositivo Móvil de Telepresencia en la Educación a Nivel Universitario, 2014).

Una experiencia muy interesante, en cuanto a la implementación del proyecto "Profesor Avatar", fue el denominado "I Challenge" donde, a través de nuestro modelo, cinco universidades de Guatemala, Perú, Chile y México se conectaron en un desafío de sostenibilidad (ver figura 2). El reto consistió en construir un generador de electricidad sostenible con materiales reciclados y, para ello, los alumnos recibieron tutoría remota a través del modelo "Profesor Avatar". Al final, los productos fabricados por los estudiantes fueron donados e instalados en áreas vulnerables de cada región (Luévano Belmonte, Telepresence technologies to humanize distance education, 2017).

6. Premios QS

El 6 de diciembre del 2016, el modelo de telepresencia "Profesor Avatar" recibió la medalla de plata en la categoría de Mejor uso de las herramientas TIC, en la edición Educación de Reimagen 2016 organizada por QS Stars y la Universidad Warthon de Pennsylvania.

Figura 2: proyecciones holográficas sobre vidrio (de Zacatecas), estación holográfica (Chile) y robots de control remoto (Guatemala y Perú), estableciendo la comunicación entre múltiples estudiantes de América Latina que se transmiten desde la ciudad de Monterrey.
Fuente: expuesto por el autor.

Esta distinción reconoció a la iniciativa como uno de los proyectos más innovadores del mundo diseñados para mejorar la pedagogía y la empleabilidad de los estudiantes universitarios. El concepto detrás de los Premios de Educación de Reimagen señala que la educación tradicional es insuficiente y excesivamente costosa para las necesidades de los estudiantes modernos y, por lo tanto, debe reinventarse (StarMedia, 2016).

Luego que el proyecto "Profesor Avatar" ganase la medalla de plata en dicho certamen, debido al desarrollo de tecnología de proyección holográfica, la iniciativa se lanzó como un cohete fuera de México en el año 2016, al proporcionar holografías a cinco universidades en tres continentes. De este modo, Green Shoots y Profesor Avatar colaboraron con el uso de la tecnología holográfica en la educación sudafricana y la primera aplicación en el nivel K-12.

7. Métodos experimentales (si existiese alguno)

El enfoque pedagógico utilizado en esta experiencia fue el aprendizaje basado en los desafíos y el aprendizaje activo, a través del uso innovador de la telepresencia, que permitió gestar esfuerzos internacionales en cuanto a la colaboración con el proyecto. Asimismo, los estudiantes fortalecieron las competencias clave para su empleabilidad y una gama de conocimientos valiosos para implementar mejoras en sus comunidades.

A través del modelo de telepresencia, los estudiantes de cuatro países colaboraron en la construcción de un generador de electricidad sostenible. Por otro lado, la metodología investigación-acción se utilizó también para recopilar información y datos consistentes en una introspectiva colectiva realizada por los participantes en situaciones sociales, con el objetivo de mejorar la racionalidad y la justicia de sus prácticas sociales o educativas, así como la comprensión de las mismas y las situaciones en las que tienen lugar.

Esta forma de investigación enlaza el enfoque experimental de las ciencias sociales con programas de acción social, los cuales responden a los principales problemas sociales. Debido a que dichas problemáticas surgen en un contexto habitual, la investigación-acción inicia el cuestionamiento de los fenómenos desde dicha arista, viajando sistemáticamente, hasta el plano filosófico. A través de este método, se pretende tratar, de manera simultánea, el conocimiento y los cambios sociales, de modo que la teoría y la práctica se unan. Si nos fijamos en la figura 3, apreciaremos la característica antropomorfista en la que el estudiante ve al profesor en escala humana real, por lo que asume que él o ella están realmente presentes en el recinto de estudio.

Por otra parte, los estudiantes que participaron en el "I-Challenge" recibieron una encuesta para que reseñarán sus opiniones en base a la experiencia vivida. De este modo, se concluyó que el 89% de los estudiantes percibió al maestro como real y sintió confianza en él, mientras que el 80% de los estudiantes consideró aceptable la retroalimentación del profesor y el 93% de los estudiantes afirmó que recomendaría el uso del modelo de telepresencia

Figura 3: proyección holográfica de un profesor del campus de Zacatecas proyectado en el campus de Monterrey.
Fuente: expuesto por el autor.

(Luévano Belmonte, Telepresence technologies to humanize distance education, 2017).

Hoy en día, el compromiso de hacer del "Profesor Avatar" una experiencia más humana y accesible es mucho mayor. A través de este modelo, es posible llevar educación de calidad a lugares que no son fácilmente accesibles, debido a circunstancias geográficas, costos o inseguridad.

En cuanto a los resultados de los instrumentos analizados para demostrar el impacto del proyecto, se tiene lo siguiente:

- El 87% percibió la proyección holográfica como la presencia social de su profesor.
- El 86% de los estudiantes estaban satisfechos con el proyecto.
- El 88% de los estudiantes se sintieron cómodos con el "Profesor Avatar".
- El 93% recomendaría este modelo a otros estudiantes.
- El 97% volvería a participar en proyectos de telepresencia.

8. Resultados de impacto

Durante la semana uno de "I-Challenge", los estudiantes construyeron un generador eléctrico sostenible utilizando material reciclado útil, con el objetivo de resolver la necesidad de una comunidad local en situación de pobreza. Cabe mencionar que enfrentarse a un problema real en una comunidad promueve la conciencia del compromiso social de los estudiantes, permitiéndoles relacionar el aprendizaje teórico del aula con la práctica, trabajar en colaboración y desarrollar habilidades respecto a la toma de decisiones, comunicación y liderazgo (Luévano, 2017).

Por otro lado, la encuesta aplicada al final del proyecto mostró los siguientes resultados:

a. El 100% de los estudiantes consideró que la telepresencia contribuyó a la mejora del aprendizaje.

b. El 87% estimó que se cumplió el objetivo de la actividad.

c. El 97% afirmó que se desarrollaron nuevas habilidades.

d. El 98% consideró que el "I-Challenge" ayudó a involucrarlos en su realidad social, económica y ambiental.

9. Conclusiones y recomendaciones

- La tecnología de proyección holográfica tiene un gran futuro por delante. A medida que esta exhibición audiovisual continúe obteniendo credibilidad de alto perfil, es probable que veamos a más empresas anunciando sus productos o comercializando sus negocios de esta manera.

- Los proyectores holográficos en desarrollo podrían ser mucho más pequeños y portátiles que los proyectores de imágenes que dependen de haces de luz convencionales. En última instancia, los proyectores holográficos pueden volverse lo suficientemente pequeños como para ser incorporados a los teléfonos celulares de futuras generaciones.

- Los proyectores podrán generar imágenes nítidas desde dispositivos de proyección relativamente pequeños (por ejemplo, teléfonos celulares) porque no requieren fuentes de luz de alta intensidad y temperatura. En ese sentido, los investigadores de las empresas y universidades están trabajando hacia la ciencia aplicada, lo cual podría devenir en un modo de hacer televisión mediante proyecciones holográficas tridimensionales en movimiento y fuera de la pantalla (Elmorshidy, 2010).

- Las tecnologías, como la realidad virtual y aumentada, están allanando el camino para la comunicación

holográfica, pero aún se encuentran en fase de desarrollo. Asimismo, se estima que en los próximos cinco años habrá un avance significativo en este campo. Por otro lado, se cuenta con una gran oportunidad en esta área, en cuanto a la capacidad de hacer este sistema lo más portátil y compacto posible, ya que su uso óptimo depende de varios factores como el espacio, iluminación y el empleo de equipo adecuados.

Referencias

Elmorshidy, A. (2010). Holographic Projection Technology: The World is Changing. *Journal of telecommunications*. 2(2). 104-112.

Luévano Belmonte, L. E. (2017). Telepresence technologies to humanize distance education. Recuperado de: http://observatory.itesm.mx/: http://observatory.itesm.mx/edu-bits-2/2017/8/28/telepresence-technologies-to-humanize-distance-education

Luévano Belmonte, L. E., López de Lara, E., & Edward Castro, J. (2015). *Use of Telepresence and Holographic Projection Mobile Device for College Degree Level*. International Conference Virtual and Augmented Reality in Education (pp. 339-347). Monterrey: Elsevier.

Luévano, L. E. (2017). Home: Profesor Avatar. Retrieved from Profesor Avatar Telepresence Model. Recuperado de http://www.profesoravatar.com

Luévano, L. E., & López de Lara, E. (2014). *Uso de Dispositivo Móvil de Telepresencia en la Educación a Nivel Universitario*. Congreso Iberoamericano de Ciencia, Tecnología, Innovación y Educación (pp. 1-12). Buenos Aires: OEI.

Luévano, L. E., López de Lara, E., & Castro, J. E. (2015). *Use of Telepresence and Holographic Projection Mobile Device for College Degree Level 015*. International Conference Virtual and Augmented Reality in Education. 75, pp. 339-347. Monterrey: Elsevier.

Minsky, M. (2010). Marvin Minsky's Telepresence Manifesto. Recuperado de http://spectrum.ieee.org/robotics/artificial-intelligence/telepresence-a-manifesto

StarMedia. (2016). Obtienen Profesores del Tec de Monterrey Tres Premios en Reimagine Education. Recuperado de www.starmedia.com: http://www.starmedia.com/noticias/obtienen-profesores-tec-monterrey-tres-premios-en-reimagine-edu/

SESIÓN 4.2

Calm.(r)
José Karlo
Jara Schenone

Es un honor dirigirme a ustedes, como moderador de este tema referido a la inteligencia artificial aplicada al ámbito de la seguridad y defensa.

Debo confesarles que hablar sobre esto trae a mi memoria recuerdos de hace 30 años atrás, en la década de los ochenta, época en la que me desempeñé como cadete en la Escuela Naval del Perú, en la primera mitad, y los años restantes como joven oficial de la Marina. Recuerdo especialmente un gran proyecto de IA denominado como la Quinta generación de computadores.

Había mucho entusiasmo, gran cantidad de reportes e información que eran publicados semanalmente en revistas de divulgación informática, a las cuales tuve acceso durante mi etapa de cadete. En 1988, ya como oficial cursante de la Escuela de Calificación de Electrónica y Comunicaciones, animado por este tema elegí desarrollar, en mi monografía final, ciertos planteamientos acerca de la aplicación de la inteligencia artificial en el proceso de decisiones de comando y control.

A medida que desarrollaba las actividades de investigación, me di cuenta de dos cosas: la primera fue que no todos los contenidos que se publican en una revista de divulgación o de noticias (a veces impulsado por gente dedicada al mercadeo) sobrevive a la rígida disciplina de una revista académica, fuente básica para los trabajos de investigación. Lo segundo que aprendí, al tratar de modelar los complejos circuitos de toma de decisiones, fue que en el colegio debí haber prestado más atención al curso de filosofía—recomendación

que también me daba mi difunto padre— ya que la toma de decisiones efectivas guarda relación con el conocimiento que se posee y el que se puede tener, siendo aspectos que la epistemología y la ontología tocan de alguna forma.

Al leer las revistas académicas y de divulgación, me di cuenta que el entusiasmo se había frenado, por lo que no obtuve suficiente información para sostener académicamente el tema, así que me vi en la obligación de reducir el alcance y concentrarme en ciertas partes del proceso de toma de decisiones de comando y control. Si alguna vez se han visto en la situación de elegir un tema de monografía o tesis, para luego darse cuenta que no hay mucha información y, por tanto, resulta necesario reducir o cambiar de tema con urgencia, reconocerán la sensación que tuve en esos tiempos.

Asimismo, el proyecto de la Quinta generación de computadores quedó descontinuado, sin haber alcanzado sus objetivos. Esto se debió, entre otras razones, por problemas de representación del conocimiento y manejo del lenguaje para la aplicación de inteligencia artificial. Años después, me enteré que, durante mi etapa de cadete, estuve leyendo reportes y noticias en el marco de lo que se denominó la “Primavera de la inteligencia artificial”, periodo de gran entusiasmo y financiamiento. Fue por eso que, apenas egresé como oficial y tras mi paso por la Escuela de Calificación en 1988, me encontré buscando información durante un periodo de “Invierno de la inteligencia artificial”, en el cual el entusiasmo chocó con ciertos aspectos de la realidad, por lo cual muchos proyectos y fondos de financiamiento fueron cancelados. Aún recuerdo la calidez de esa primavera y la preocupación de aquel invierno.

Han pasado casi treinta años de investigación, treinta años de desarrollo en el campo de la neurobiofísica para entender el funcionamiento del sistema nervioso y la

forma en la que el ser humano procesa información; han transcurrido treinta años de algorítmica para modelar en base a prototipos matemáticos, así como el desarrollo de la matemática, treinta años de investigación sobre el lenguaje humano, ingeniería lingüística y procesamiento de lenguaje natural. Por ello , la inteligencia artificial se encuentra disponible para apoyar en la toma de decisiones y, en algunos casos, para decidir aun con las discusiones morales y éticas que eso conlleva.

En tal sentido, la inteligencia artificial actual puede apreciarse cotidianamente en las rutinas de los videojuegos, cuando estas simulan el comportamiento de un oponente, en los sistemas de recomendación para ventas cruzadas en algunos sitios web comerciales, en los sistemas de predicción de pago de préstamos comerciales, con la capacidad de generar una tasa de interés personalizada en función al riesgo que los algoritmos calculen.

Es en este contexto en el cual buscamos aplicaciones de inteligencia artificial en el área de seguridad y defensa, y dado que en este campo se encuentra implícita, de una u otra forma, la aplicación de violencia contra personas, los aspectos éticos y morales tienen una importancia capital. Cabría preguntarnos entonces hacia dónde vamos, pues bien, es aquí donde entran en juego los temas que nuestros expositores sostendrán hoy.

Por un lado tenemos al Doctor William Bundy, que a lo largo de una exitosa carrera como oficial de la Marina de los EEUU, con énfasis en las operaciones submarinas, nos señalará las oportunidades en las que hubieran podido aplicarse técnicas de inteligencia artificial, así como las posibilidades existentes hoy. Asimismo, en esta ocasión nos presentará una visión de la IA hacia el futuro, específicamente en el año 2050, periodo en el que las líneas de desarrollo de la IA estarán conectadas a las técnicas de la robótica. En la actualidad, el Dr. Bundy se

desempeña como decano asociado de Investigación y Desarrollo de Combate en la U.S. Naval War College.

Por otro lado tenemos al licenciado José Ángel Gallego, matemático de profesión que nos dará una presentación sobre la aplicabilidad actual de la IA, desde su experiencia como director de la empresa Everis Aeroespacial y Defensa. Específicamente, nos presentará el estado del arte de la IA, para luego mostrarnos dos aplicaciones conectadas con el empleo de plataformas UAV.

sesión

4.2

La cuarta era: la revolución en robótica e inteligencia artificial en la guerra

Dr.
William F. Bundy

Antes que nada, deseo transmitirles el saludo de nuestra presidenta, la Contralmirante Shoshana Chatflied, y de nuestra facultad. Sé que algunos de los presentes son graduados de la U.S. Naval War College y que aquí en Perú cuentan también con su propia Escuela Superior de Guerra Naval, la cual provee educación sustancial, gestión y dirección a sus fuerzas navales.

Mi intención es hablarles acerca del futuro, el cual ocurre en este preciso momento. Hemos recorrido un largo camino desde los albores de las operaciones mecánicas, hasta el establecimiento de la automatización, proceso que permite a las máquinas realizar funciones que anteriormente eran desarrolladas por humanos. Asimismo, este mecanismo hace posible ejercer labores de comando y control, especialmente de los sistemas automáticos, pasando por los robots hasta los vehículos autónomos submarinos. Todo esto es utilizado en la actualidad, por lo que resulta necesario analizar la aceleración de los avances tecnológicos hacia el futuro.

En ese sentido, he leído mucho sobre el tema en los últimos años y trabajado muy de cerca con el U.S. Naval Undersea Warfare, donde nuestros científicos crean escenarios de guerra para la Armada, describiendo una serie de puntos a tomar en cuenta. Por otro lado, trabajé con la U.S. Naval Surface Service, institución que cuenta con ingenieros y científicos que visualizan la operación de distintas unidades de superficie con sistemas de misiles. Es por ello que contamos con escenarios navales específicos: uno en la parte de la costa del Atlántico y otro donde se realizan trabajos con un grupo de ingenieros.

No obstante, es preciso entender la aplicación de nuestros valores y filosofía para la operación de las fuerzas: estas deben ganar las guerras que aparezcan, pero lo más importante es demostrar su poderío para evitarlas. A lo largo de los años, hemos visto operar a flotas que poseen un gran poder, sin embargo, hoy en día surge una gran

discusión en torno a la capacidad que deben poseer los oficiales técnicos, respecto al manejo de las mismas. En mi opinión, creo que los británicos resolvieron este problema, debido a que tenían oficiales ingenieros en sus filas, a diferencia de los Estados Unidos, en donde historiadores o ingenieros cumplían con dicho papel.

En tal sentido, nos encontramos en un punto de inflexión, en el que la tecnología está acelerándose y es adaptada por la sociedad. Esto es lo que llamaría — y tomo este lenguaje de Byron Reese—, el advenimiento de una cuarta era, referida a la evolución tecnológica.

La cuarta era: la revolución en robótica e inteligencia artificial en la guerra

Dr. William F.Bundy, Director Asociado de Investigación y Desarrollo de la Guerra

Byron Reese ofrece una descripción de nuestra entrada en la Cuarta Era de la Evolución Tecnológica. Esa evolución cultural está siendo llevada por la adopción de robots inteligentes, computadoras conscientes y una sociedad que llegará a depender de y demandar tecnologías que provean acceso inmediato a bienes, servicios y conocimientos. Nuestra Cuarta Era transformará cada aspecto del esfuerzo humano incluyendo la guerra. Según Reese, "la tecnología ha cambiado la cara de la guerra docenas de veces en los pasados pocos cientos de año... los robots y AI la cambiarán de nuevo".

¿Cuáles son las posibilidades y cómo los ejércitos y las marinas emplearán sistemas y armas autónomos a lo largo de las fases de las operaciones militares? ¿Cuáles son las posibilidades para el equipo entre humano y máquina y el desarrollo de elementos militares inteligentes en tiempos de paz y en guerra? ¿Cuáles son las ventajas y consecuencias de las fuerzas marítimas autónomas que operen en el mar?

Estas preguntas surgirán durante la evaluación para adoptar innovación militar y marítima en la Cuarta Era.

Figura 1: la cuarta era: la revolución en robótica e inteligencia artificial en la guerra.
Fuente: expuesto por el autor.

A continuación, intentaré sustentar esta premisa. En esta ilustración observamos la producción de uno de nuestros contratistas más importantes; se trata de un submarino hostil, en el cual apreciamos armas que operan a través de un sistema de control automatizado, el cual utiliza la inteligencia artificial mediante una especie de red neuronal.

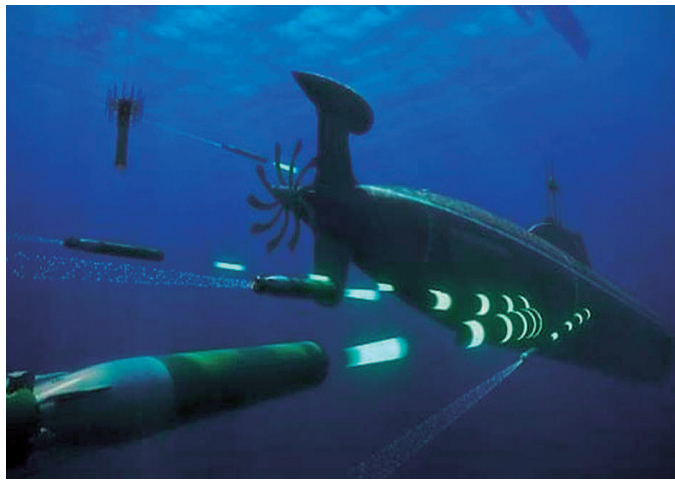


Figura 2: la cuarta era de la evolución tecnológica es transformar la sociedad y la guerra
Fuente: expuesto por el autor.

Por otra parte, sobre el océano se desplazan helicópteros con sonares que tienen la habilidad de monitorear y mantener contacto con el submarino, así como también encontramos embarcaciones no tripuladas que pueden utilizarse para los mismos propósitos; como verán, la era de la evolución tecnológica se revela ante nuestros ojos.

Ahora bien, quisiera preguntarles cuántos de ustedes tienen un *smartphone*. Hace diez años, era imposible pensar en el uso masivo de estos aparatos. En la actualidad, solemos buscar en Google términos que no entendemos, lo que significa recibir información de forma inmediata. De igual modo, si queremos hablar con algún amigo, podemos llamarlo en cualquier momento. Ustedes recordarán aquel show televisivo en el que se respondían preguntas y cuyo anuncio era: sí quieres responder, puedes llamar a alguien. En efecto, somos capaces de llamar a cualquier persona mediante estos dispositivos, los cuales nos brindan acceso ilimitado a juegos, videos, entre otras aplicaciones; la tecnología está en nuestras manos.

Estoy seguro que muchos de los aquí presentes conocieron el *Blackberry*, que fue un teléfono celular en el que se recibían correos electrónicos, así como también los celulares a los que solíamos llamar "ladrillos", debido a que eran de gran tamaño y poseían una antena larga. Ante ello, Steve Jobs, creador de Apple, y su equipo vieron la posibilidad de fusionar esta tecnología y las capacidades propias de una computadora, para colocarlas en un dispositivo. De este modo, mezclaron las capacidades del Ipad con la música y luego con el Iphone.

Esto quiere decir que la tecnología puede ser desarrollada por un grupo específico de personas. Entonces, una vez revelada hacia el mundo, todos intentan hacerse con la novedad tecnológica. Este fenómeno es común en la actualidad.

Figura 3: era de revolución en asuntos militares.
Fuente: expuesto por el autor.

En esta imagen, mucho de lo que observan ha sucedido o está a punto de ocurrir. En tal caso, cabría preguntarse cuál es el motor que propulsa esta era de evolución tecnológica. Hemos hablado de la inteligencia artificial, pero a mí me

gustaría llamarla como la era de la inteligencia, ya que es posible dar órdenes a las máquinas y que estas procedan conforme a estas. Tengamos en cuenta que la capacidad más poderosa en este campo es el trabajo conjunto entre la sociedad y las máquinas; esto es lo que comúnmente llamamos *quantum*, lo equivale a referirnos al misterio mismo de la ciencia.

A menudo, al referirnos a la mecánica cuántica, evocamos la idea de una serie de partículas operando al mismo tiempo y en la misma fase. A simple vista, pareciera que fuese algo complicado, pero déjenme decirles que es posible separar estas partículas y actualizarlas de forma idéntica; esto significa que debemos utilizar esta mecánica para mejorar.

Por otro lado, les hablaré sobre la robótica y la automatización, desde el punto de vista en el que uno es capaz de elaborar un prototipo capaz de realizar operaciones, trabajos y tareas, al igual que un humano. Sin embargo, es preciso separar esta idea del concepto de la autonomía, ya que supone el hecho de operar y controlar un sistema específico.

Figura 4: BAE Systems.
Fuente: expuesto por el autor.

En la actualidad, la corporación BAE Systems produce sistemas que operan con inteligencia artificial, mediante el uso de la realidad virtual, siendo esta tecnología puesta a disposición de los usuarios. En esta realidad, es posible ofrecer un mejor entendimiento de lo que se está haciendo, gracias a la proyección virtual del ejecutor de la acción; por ejemplo, si un técnico se encuentra montando una parte mecánica, o si está buscando algo en el mar, se podrá tomar esta información desde la inteligencia artificial.

Veamos ahora el caso de una embarcación. En primera instancia, es posible saber su nombre y la velocidad de navegación que emplea (datos que dan al operario mayor conocimiento del entorno). De hecho, hace poco fui partícipe de una discusión acerca de cuanta tecnología debe suministrarse a un oficial respecto a este punto ; con ello, volvemos al enfoque tradicional, en el cual tendremos que maniobrar la embarcación de manera autónoma, entendiendo los alcances de cada acción. Bien sabemos los presentes que cada oficial que se adentra en el mar debe tener muy claros estos fundamentos.

Sin embargo, es posible automatizar muchos de los procesos de navegación y utilizar la inteligencia artificial, hasta el punto en que no se necesite de ningún tripulante a bordo para realizar operaciones. Por ello, es necesario que la máquina y el humano trabajen en forma conjunta. Las máquinas tienen la capacidad de calcular y comparar más rápido que cualquiera de nosotros, de hecho, una persona es capaz de comprender el ambiente operacional o entender la situación táctica de una nave; esto quiere decir que, en términos de maniobras y ataque, la máquina puede efectuar acciones mucho más rápidas que un humano, en consecuencia, el operario debe recibir las opciones resultantes del trabajo mecánico.

Y ya que hablamos de realidad virtual, es probable que hayamos visto algunos ejemplos. Sabemos que una

persona, ubicada a kilómetros de distancia, puede ser proyectada dentro de esta sala. Sin embargo, podemos utilizar esta tecnología para efectos de capacitación y formación, por lo que cualquiera de nosotros podría manipular una situación dentro de un ambiente virtual; supongamos que un torpedo es lanzado, entonces, a partir de la realidad virtual, seremos capaces de maniobrar la nave, en respuesta al ataque en curso. En tanto, es importante entender que esa realidad conlleva a que el oficial reconozca que se encuentra en un escenario de guerra. Por eso, cuando observamos estas imágenes tridimensionales de una operación común, el entendimiento del uso de la tecnología ofrece la real magnitud de la situación.

En una parte del libro *"The Entanglement"*, se menciona que hay un sistema de computadora operando en una nave y, de pronto, esta le dice al comandante que debe tomar una decisión, a lo que responde que, debido a la confianza que le tiene, dejará en sus manos el poder decisor. En tanto, la computadora se niega a hacerlo, puesto que es una decisión que debe ser tomada por un ser humano; en ese momento, el comandante se levanta y acude a la sala de mando, mientras la computadora lo pone al tanto de la situación. Me detendré en este punto, pues es mi deseo que ustedes tengan la feliz experiencia de leer esta obra y observar el proceso tecnológico. A propósito, es una serie muy interesante, compuesta por tres libros. El primero es *"The Entanglement"*, seguido de Entropía y de Evolución. Estoy seguro que será una lectura muy interesante para ustedes, ya que les dará un amplio panorama sobre el futuro, la inteligencia artificial y la realidad virtual.

Aquí tenemos a un equipo alrededor de la mesa de ploteo, tecnología que puede ser usada de manera inteligente, en el sentido que podría brindar opciones mucho más precisas, a diferencia de las que ustedes y yo conocemos. Por otro lado, tenemos oficiales subalternos que envían toda la información al Centro de Operaciones de Combate.

Figura 5: la tecnología de agente inteligente.
Fuente: expuesto por el autor.

Ese operario, que trata de entender el vuelo de una nueva aeronave al mirar los radares, intenta comprender la información recibida, en términos de alertas; pero debemos saber que, a nivel táctico, desde las maniobras, hasta los niveles de comando, todas las acciones serán ejecutadas por los sistemas de inteligencia artificial en los futuros escenarios de combate. A su vez, estas herramientas realizarán la gestión combativa, proporcionarán los cursos de acción a nivel operacional, las decisiones tácticas a nivel de maniobra y el compromiso de las decisiones a nivel táctico.

Con el paso del tiempo, la inteligencia artificial y las computadoras entablarán un proceso de comunicación, formando una red que nos brindará información precisa para ser trabajadas a lo largo de las redes, gracias a la producción devenida de la IA. Ese es el futuro y habitaremos allí hasta que consigamos otras alternativas de desarrollo.

Ahora bien, les comentaré algo acerca de la inteligencia artificial. Existe una serie de definiciones respecto a ella,

pero en mi opinión considero que, para conseguir un concepto exacto, es preciso observarla desde el punto de vista de las ciencias de la computación y la informática, ya que es una capacidad evolutiva que, en muchos casos, es comparada con acciones basadas en la observación de la información. De sobra sabemos que las computadoras IBM son capaces de ganarnos en una partida de ajedrez, debido a que su desarrollo involucra movimientos mecánicos; estas máquinas son capaces de almacenar cientos de movimientos y pueden comparar lo observado en la última movida, para obtener mejores resultados en las siguientes jugadas. Eso es inteligencia artificial, *machine learning*, computación en evolución, hoy en día, informática involutiva.

Figura 6: elementos de la Inteligencia Artificial.
Fuente: Razón Social.

Me permito hacer un paréntesis en este punto, pues esta semana escuché, en diversas ponencias, hablar acerca de la visualización, comunicación de lenguajes naturales y temas relacionados a la cibernética. En tal sentido, les comento que estuve involucrado en la transición a la banca en línea, en una parte de mi carrera. Cuando empezamos ese proceso, supimos de antemano que podíamos proporcionar a nuestros clientes una serie de

opciones, como cancelar sus cuentas, transferir dinero instantáneamente, entre otros servicios.

Asimismo, nuestra mayor preocupación radicaba en que un hacker penetrase en los sistemas y se llevase el dinero de nuestros clientes; en ese momento no le llamábamos cyber, sino robo informático. De este modo, entendimos que el usuario promedio no emplea los protocolos de seguridad necesarios para proteger sus cuentas, por ejemplo, muchos de ellos no procedían de forma correcta al establecer sus claves, lo que ofrecía una vulnerabilidad apetitosa para cualquier atacante. Por otro lado, teníamos pleno conocimiento de que algunas personas procederían de forma ilegal, al estar motivadas por la sustracción de dinero, lo que hoy en día conocemos como crimen cibernético. Dos de mis colegas ofrecieron un panorama muy bueno sobre eso, pero quiero que entiendan estas cuestiones acerca del cyber.

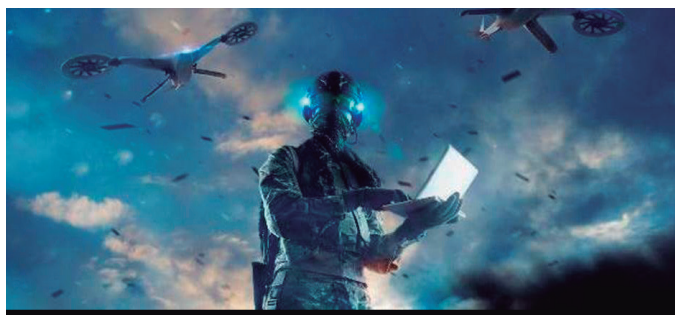
Muchas veces empleamos los términos ciberdefensa o ciberoperación, pues bien, esto que plantearé a continuación será una extensión de lo que estoy hablando, ampliando un poco más el concepto de quantum. Esta semana leí un artículo en el que se contaba que alguien intentaba crear un nuevo tipo de internet en el que, en vez

Figura 7: el quántum - computadoras, sensores y comunicación.
Fuente: Fiona Macdonald - www.sciencealert.com

de transmitir información en 0 y 1, se hiciese utilizando q-bits, herramienta de la mecánica cuántica que permite que una expresión sea 1 y 0 al mismo tiempo, lo que ofrece mayor flexibilidad y maniobrabilidad.

Asimismo, mencioné el término *entanglement*, que es la legitimización en la separación de partículas que operan como gemelas, no importando donde se encuentren. Toda esa capacidad tiene grandes implicancias, por ejemplo, en cuanto a si el siguiente gran descubrimiento será inmediato o si tomará diez años en ser revelado . Con esto pretendo que ustedes reconozcan que en sus carreras notarán diversos descubrimientos a diario, los cuales acelerarán la tecnología que ustedes reciben. De esto trata la comunicación cuántica, la encriptación cuántica y las computadoras avanzadas en esta mecánica. Y todo esto, mis queridos colegas, está llegando muy rápido hacia nosotros.

En esta lámina tenemos a un guerrero operando una serie de drones, los cuales pueden ser dirigidos a través de un dispositivo en el que el operador debe tomar muchas decisiones; o bien se podría dirigir este drone a través de la inteligencia artificial, de modo que la máquina recibirá



Control de Tiro: cálculos informáticos a la velocidad de la máquina, automatización del control y el empleo.

Figura 8: India trabaja en tanques, embarcaciones y armamento robótico no tripulados.
Fuente: Colin Anderson a través de Getty Images.

información de la misión e instrucciones, a fin de generar entradas adecuadas al sistema de control, para maniobrar el drone. Esto se da en un rango operativo, a control remoto, semiautomático o totalmente automático.

Esta nave es el Sea Hunter, en la cual estuve abordo y en donde recordé a los submarinos diésel, los cuales tienen compartimentos llenos de sistemas electrónicos y que están configurados con diferentes características (a diferencia del Sea Hunter que opera de manera autónoma).

Figura 9: un "Cazador del Mar", vehículo no tripulado, llega a Honolulu después de un tránsito autónomo desde California, 2018
Fuente: Marina de los EE.UU.

Figura 10: modos de operación: control remoto, semiautónoma y completamente autónoma.
Fuente: Devin Coldewey@techcrunch.

Esta embarcación ha navegado de San Diego a Pearl Harbor de manera satisfactoria, operando con capacidades semiautónomas y sin tripulación.

En algún momento, los pilotos de aeronaves se quedarán sin trabajo, dado que estas serán no tripuladas. Otro tipo de nave submarina no tripulada se llama Echo Voyager de Boeing, que es una nave de 51 pies utilizada para fines comerciales y militares, lo que evidencia que la Marina de Estados Unidos está aceptando el uso de naves no tripuladas.

Figura 11: el Echo Voyager de Boeing de 51 pies de largo puede pasar seis meses planeando por el océano.
Fuente: BOEING.

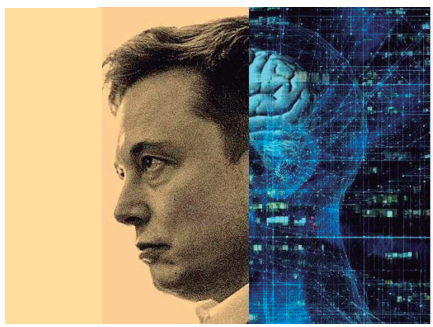
La tripulación del barco estaría compuesta por alrededor de 50 a 100 marineros, en lugar de los 200 tripulantes que se encuentran en los buques de guerra de hoy, con el centro neurálgico del barco, la Sala de Operaciones, con cinco personas en lugar de 25.
(El *Diplomat* y *Startpoint* 2015)

El *Dreadnought* 2050 también estaría equipado con "tubos de misiles para misiles hipersónicos defensivos (es decir, *Mach 5 plus*), armas de energía dirigida para detener pequeñas naves enemigas cargadas con explosivos; y en las armas (los cascos de los estabilizadores) habría tubos de torpedos para disparar torpedos supercavitantes capaces de desplazarse a más de 300 nudos".

Figura 12: el Dreadnought 2050.
Fuente: expuesto por el autor.

Por otro lado, el Dreadnought 2050 es una nave de control marino que contará con una cantidad de cincuenta a cien tripulantes, a diferencia de los buques actuales en los que su centro de operaciones de combate solo contará con cinco personas. Esta nave también estará equipada con misiles supersónicos de defensa, armas de energía dirigidas para destruir amenazas asimétricas y tubos lanzatorpedos que dispararán torpedos de supercavitación de más de 300 nudos.

Al hablar del proceso de integración entre el hombre y la máquina, Elon Musk ofrece la visión de utilizar interfaces cerebro-computadora, para controlar smartphones (imagínense usar aplicaciones y escribir mensajes de texto sin emplear los dedos), considerando que tecnologías como las de Neuralink podrían convertirse en herramientas de vanguardia para la medicina y la cirugía.



Elon Musk visualiza el uso de interfaces de cerebro y computador (BCI), para controlar teléfonos inteligentes, imagina usar una aplicación o escribir un mensaje de texto sin mover los dedos,pero tecnologías como la de *Neuralink* también podrían convertirse en herramientas innovadoras para la medicina y la cirugía. [Comandantes, personal y operadores con amplios recursos de datos].

Figura 14: Elon Musk
Fuente: Lucille M. Tournas y Walter G. Johnson,State.

Finalmente, tenemos que entender que la tecnología puede hacer mucho, pero debemos estar seguros en cuanto al control que podamos tener sobre ella. No sea que, en algún momento, ese control pase de las máquinas hacia nosotros.

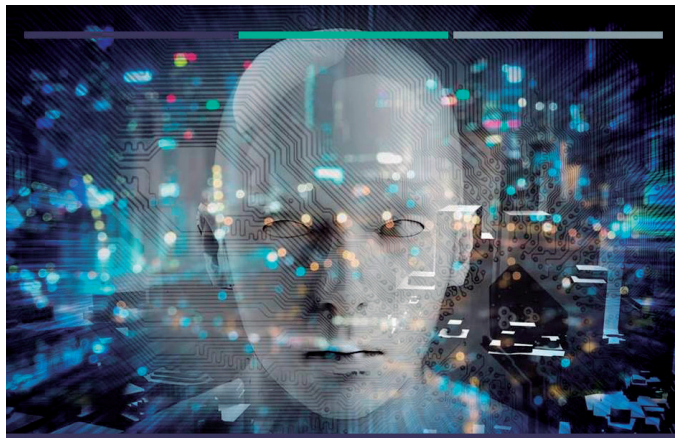


Figura 15: inteligencia artificial.
Fuente: Getty Images/iStockphoto.

sesión

4.2

Inteligencia artificial aplicada a los UAVs

Lic.
José Angel Gallego

La inteligencia artificial (IA) es una tecnología disruptiva y trasversal que está transformando todos los sectores industriales, sin excepción. Los sistemas autónomos, en particular los UAS (Unmanned Aerial System), son un claro ejemplo de ello, ya que hay amplios campos de aplicación de esta tecnología, desde las propias capacidades de navegación autónoma, hasta el consumo y explotación en tiempo real de la información recogida por los sensores embarcados.

Se podría decir que fue en la década de los noventa (y con una aplicación claramente militar) cuando se empezó a introducir técnicas de inteligencia artificial en el desarrollo del Predator UAV, durante la guerra de los Balcanes. Desde entonces, gracias al desarrollo exponencial de la tecnología asociada a los UAVs[1] y su universalización, se viene produciendo la eclosión de una infinidad de aplicaciones, desde capacidades avanzadas de navegación sin dependencia de sensores GNSS[2], hasta el tratamiento a bordo y en tiempo real de las imágenes recogidas por las cámaras embarcadas. Estas aplicaciones tienen un claro empleo tanto en el ámbito civil como en el militar.

Una vez revisado el estado del arte para aplicaciones como la navegación en exteriores, o para el levantamiento y clasificación de objetivos en tiempo real, será importante también conocer cuáles son las limitaciones actuales y los principales retos que debe enfrentar, en un corto y medio plazo, el desarrollo de esta tecnología en el campo técnico, ético y moral.

Palabras clave: Inteligencia artificial; *Machine Learning*, *Deep Learning*; fusión de sensores; navegación por visión; sistemas no tripulados; drones; UAV; GNSS degradado o denegado.

1. Introducción

Se conoce como inteligencia artificial a aquella capacidad desarrollada por máquinas capaces de ejecutar y aplicar

NOTA

[1] UAV: Unmanned Aerial Vehicle
[2] GNSS: Global Navigation Satellite System

algoritmos y estadísticas, para la resolución de problemas y ejecución de tareas, mediante la emulación de la inteligencia humana. Se trata de un área multidisciplinar que estudia el diseño y la creación de entidades capaces de realizar tareas por sí mismas, a través de disciplinas como la computación, la lógica, la filosofía, la matemática computacional y la estadística, manteniendo siempre a la inteligencia humana como paradigma en términos de percepción, razonamiento, aprendizaje, interactuación con el entorno y resolución de problemas, o incluso ejercitando su propia creatividad.

Haciendo un poco de historia, la IA emerge como disciplina en los años 50, gracias a las diferentes investigaciones llevadas a cabo durante la Segunda Guerra Mundial. De hecho, fue en 1950 cuando Alan Turing introdujo el concepto de *"Turing test"*, el cual permite medir la capacidad de una máquina que muestra un comportamiento inteligente similar al de un humano.

Desde entonces, esta disciplina ha tenido distintos altibajos relacionados con el desarrollo tecnológico y de capacidades computacionales y de procesamiento de cada época, que no permitían demostrar los avances teóricos y validar los diferentes algoritmos, los cuales requerían de una capacidad procesal inalcanzable en momentos particulares. En este contexto, el desarrollo de la IA ha ido de la mano con los desarrollos tecnológicos en materia de procesadores, memoria y capacidad computacional; como hitos destacables, cabe mencionar la derrota del campeón del mundo de ajedrez Gary Kasparov, en 1997, por parte de Deep Blue, computadora autónoma desarrollada por IBM, o AlphaZero, desarrollada por Deep Mind, que en el 2018 aprendió a jugar al ajedrez en un solo día y de forma autodidacta.

Atendiendo al desarrollo de los sistemas aéreos no tripulados (UAS) se podría decir que el punto de inflexión en la aplicación de IA a esta tecnología fue el desarrollo

del Predator, por parte de la Fuerza Aérea de los Estados Unidos, en los años 90. Asimismo, entró en servicio durante la guerra de los Balcanes en 1995 y puso en valor las ventajas operativas que ofrecen los UAVs, convirtiéndose en un activo imprescindible para el abordaje de cualquier operación militar.

Actualmente, gracias a la universalización de la tecnología y a la industrialización de componentes, ambos desarrollos están al alcance de cualquiera. De hecho, no es descabellado afirmar que, hoy en día, cualquier persona tecnológicamente avezada sería capaz de construir su propio drone y dotarlo de capacidades autónomas de navegación o incluso implementar algún tipo de tratamiento automático de imágenes, todo ello con un presupuesto muy ajustado. Además, es muy importante destacar que ya no suponen grandes barreras de entrada ni el acceso al conocimiento, ni las herramientas de desarrollo, ni los componentes. En tanto, existe gran cantidad de comunidades que producen y desarrollan nuevos algoritmos, y entrenan redes neuronales para diferentes aplicaciones, utilizando herramientas y paquetes de desarrollo *open source*, que facilitan el acceso a este conocimiento. Por otro lado, las tarjetas de evaluación están al alcance de cualquier persona, al igual que los procesadores de costes muy reducidos y con acceso a proyectos *open source* disponibles, los cuales hacen posible un primer acercamiento hacia esta tecnología.

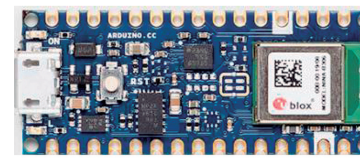


Figura 1: tarjeta arduino.
Fuente: expuesto por el autor.

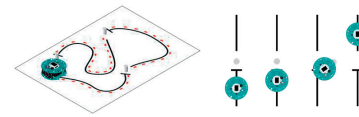


Figura 2: proyecto de robot inteligente "RobotRescue" de arduino.cc.
Fuente: expuesto por el autor.

En este contexto, las posibilidades que ofrecen las técnicas de inteligencia artificial aplicadas a los UAVs son

prácticamente infinitas, ya que hay miles de desarrolladores implementando diferentes soluciones, para distintas casuísticas y aplicaciones; aunque es evidente que cualquier aplicación destinada a los ámbitos de seguridad y defensa (o para cualquier aplicación profesional) debe asegurar ciertos parámetros de calidad, robustez, fiabilidad y seguridad, lo cual implica una importante inversión en cuanto a diseño, implementación y pruebas, acciones que tienen por objetivo ofrecer las garantías necesarias en el uso de esta tecnología.

Ahora bien, desde un punto de vista técnico, hay una serie de limitaciones para el desarrollo de aplicaciones basadas en IA para UAVs, que es importante tener en cuenta:

- Disponibilidad de sensores embarcados que ofrezcan cada vez más información precisa, a través de equipos ligeros que sean fácilmente embarcables en las UAVs.
- Es necesario implementar una fusión de sensores optimizada que combine toda la información disponible para obtener una solución más robusta y fiable, aplicando técnicas de big data.
- Es imprescindible contar con una gran capacidad de procesamiento embarcado para el tratamiento de toda la información y eso implica, a su vez, manejar soluciones de compromiso en términos de peso, consumo de energía y tiempo de proceso, parámetros especialmente sensibles cuando hablamos de plataformas UAV.
- Para este tipo de aplicaciones es fundamental disponer de una base de datos completa, acerca del caso de uso sobre el que se esté trabajando, para entrenar bien las redes implementadas. En caso de datasets incompletos o deficientes, el grado de incertidumbre reduciría considerablemente las probabilidades de éxito de la solución.

- Definir con claridad el concepto operativo de la solución para manejar, de forma adecuada, la complejidad del modelo y la arquitectura de la solución.

Estas limitaciones definen los principales retos a abordar, en el corto y medio plazo, para la aplicación y generalización de este tipo de soluciones en escenarios operativos reales, aunque con la tecnología actual ya es posible implementar soluciones muy interesantes. A continuación, se presentarán dos sistemas UAVs desarrollados por Everis Aeroespacial y Defensa, con capacidades de vuelo totalmente automatizadas, a través de un piloto automático y con capacidades ISR avanzadas, mediante el procesamiento embarcado y en tiempo real de imágenes. Se trata de sistemas sobre los que se han implementado las soluciones y casos prácticos que veremos a continuación.

Figura 3: sistema UAV de ala fija TUCÁN.
Fuente: expuesto por el autor.

Figura 4: sistema UAV cautivo ASTER-T.
Fuente: expuesto por el autor.

2. Aproximación tecnológica

Sin ánimo de hacer una aproximación exhaustiva, desde un punto de vista tecnológico es posible establecer una clasificación técnica en función a la forma de operación y de los métodos de aprendizaje, ya sean a través del entrenamiento, o bien infiriendo conclusiones en base a los datos disponibles. En este contexto, hay diferentes tipologías de algoritmos que permiten ambos métodos de aprendizaje: algoritmos de regresión, redes neuronales artificiales, algoritmos bayesianos, árboles de decisión, redes neuronales convolucionales, entre otros.

Aplicando estos algoritmos, junto con una capacidad de computación de alto rendimiento (HPC[3]) y la gran cantidad de información disponible (big data) obtenemos una arquitectura genérica de IA, la cual quedaría definida por la capacidad del proceso, la cantidad de información disponible y el uso de algoritmos eficientes. Por lo tanto, en base a la plataforma de IA empleada, aparecen dos tecnologías de aprendizaje:

Machine Learning

Este concepto refiere a una tecnología de propósito general más importante y que permite el desarrollo extraordinario de los últimos años. Asimismo, el *machine learning* consiste en la detección de patrones y el aprendizaje respecto a la elaboración de predicciones y recomendaciones, procesando toda la información disponible y las experiencias anteriores. En ese sentido, es posible clasificarlo en tres grandes grupos:

- **Aprendizaje supervisado**

  Requiere del *feedback* humano al momento de procesar información y relacionar entradas y salidas predefinidas del proceso.

- **Aprendizaje no supervisado**

  Ocurre cuando los algoritmos tratan las entradas

NOTA

[3] HPC: High Performance Computing

de información y no tienen salidas definidas, permitiendo, por tanto, la detección de patrones para la clasificación de las salidas.

- **Aprendizaje de refuerzo**

  Se trata de algoritmos que aprenden a ejecutar tareas sencillas, en base a maximizar el retorno de dicha acción, por lo que el aprendizaje se da en base al comportamiento del entorno y la interacción con él.

Deep learning

Es un tipo particular de *machine learning*, capaz de sacar provecho a un volumen mucho mayor de información, basado en una red interconectada de capas que conforman diferentes niveles jerárquicos (ANN, *Artificial Neuronal Network*) de manera que, a través de las múltiples operaciones aplicadas en cada nivel, podrá inferir algo que trasladar al siguiente nivel, para continuar con el proceso de aprendizaje y generalizar un conocimiento más complejo. En tanto, los modelos o tipos de capas más utilizados en *deep learning* son:

- **Redes neuronales convolucionales (Convolutional neuronal network)**

  Son redes basadas en la extracción de características cada vez más complejas, para determinar la salida. Asimismo, es la más utilizada en conjuntos de información desestructurada, como es el caso de las imágenes.

- **Redes Neuronales Recurrentes (Recurrent neuronal network)**

  Son aquellas que permiten almacenar información en la salida de cada nodo, lo que permite el aprendizaje a través de secuencias, siendo muy apropiadas para series de datos temporales.

Cuando se habla de inteligencia artificial aplicada a los UAVs, es fácil pensar que alguna de ellas es la óptima para el desarrollo de aplicaciones, sin embargo, es muy importante tener en cuenta todas las tecnologías y algoritmos, al momento de aproximar un problema y definir cuál es el modelo de IA óptimo, en función de la información disponible, la capacidad de proceso y el concepto operativo definido.

De esta forma, no se aplicaría la misma aproximación para el desarrollo de capacidades de un piloto automático —que debe consumir la información de todos los sensores embarcados, procesarlos y, en base a las estrategias de guiado y a las condiciones de la plataforma, calcular la salida de control más adecuada aprendiendo continuamente del entorno— que para el tratamiento en tiempo real de las imágenes capturadas por el UAV, de cara a la extracción y clasificación de los diferentes elementos de la imagen. En ambos casos, se emplean técnicas de inteligencia artificial, pero el modelo aplicado a cada una de ellas es totalmente diferente.

Por todo ello, se debe entender bien el caso de uso, la capacidad real del proceso y la información disponible para llevar a cabo un óptimo aprendizaje, que garantice resultados aceptables.

3. Caso práctico

A continuación, veremos unas pinceladas de dos proyectos I+D, llevados a cabo por Everis Aeroespacial y Defensa, los mismos que permiten poner en la palestra dos aplicaciones de técnicas de inteligencia artificial aplicada a los UAVs. Se trata de los proyectos VIDEUSS y AZOR, en el marco de los cuales se está desarrollando un sistema de IA para la detección y localización de objetivos y donde, además, se aborda una solución de navegación avanzada apoyada en la visión artificial y sin dependencia de señal GNSS.

En ambos casos, resulta de vital importancia definir una arquitectura de hardware que aporte la capacidad necesaria de procesamiento a bordo y, a su vez, permita ser embarcado en la plataforma UAV, definida en términos de peso, consumos, necesidades de integración, entre otras. Las plataformas sobre las que se han implementado estas soluciones corresponden con los sistemas TUCAN y ASTER-T presentados anteriormente y, en cuanto a la

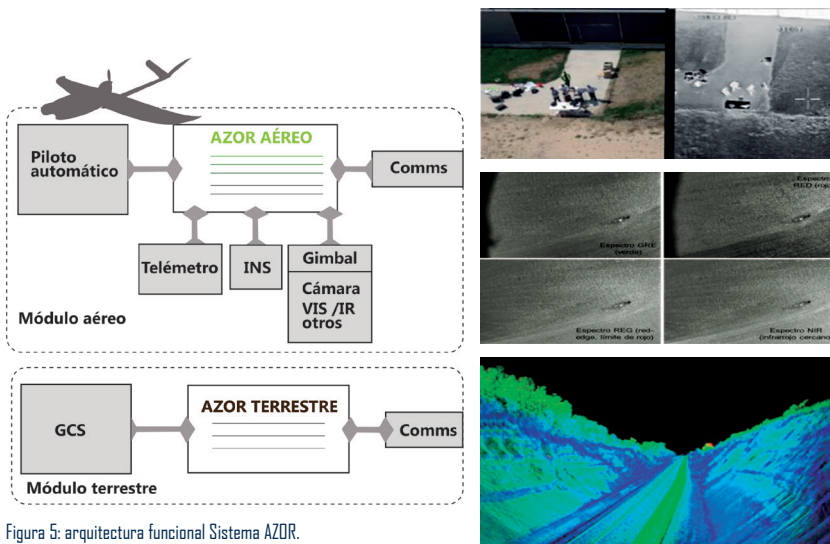


Figura 5: arquitectura funcional Sistema AZOR.
Fuente: expuesto por el autor.

configuración de hardware embarcada, se ha basado en un procesador GPU sobre el que se han integrado diferentes sensores, además de un interfaz de comunicación con el autopiloto. Por otro lado, el modelo se completa con un módulo en tierra, conectado con la estación terrestre del UAV, para la operación del sistema.

Modelo de implementación

A continuación, se describe de forma gráfica la arquitectura funcional del sistema, con una diferenciación clara entre el módulo embarcado (o módulo aire) y el módulo tierra.

Desde un punto de vista funcional, en el módulo aire podemos diferenciar los siguientes bloques:

- **Autopiloto**

  Capacidad de navegación, guiado y controlado totalmente de forma automatizada, mediante hibridación INS[4]/GNSS.

- **Sensores embarcados**

  Son sensores integrados en el sistema, que permiten ofrecer conciencia situacional. Entre ellos destacan los acelerómetros, giróscopos, telémetros, receptores GNSS y, fundamentalmente, un sensor óptico gimbalizado, para operar en un rango visible e infrarojo.

Procesador embarcado

Es un procesador que gestiona la fusión de sensores con toda la información disponible y ejecuta los diferentes algoritmos de IA en tiempo real, para cada aplicación definida, posibilitando una toma de decisiones automatizada.

En cuanto al módulo de tierra, también está integrado con la estación de mando y control del propio UAV y cuenta con capacidad de proceso, aunque sobre CPU en este caso, a diferencia del sistema embarcado que trabaja sobre GPU para disponer de mayor capacidad de proceso. Gracias a este módulo, se puede operar el sistema, manteniendo en su caso el *man on the loop*, para supervisar la toma de decisiones y ejecutar procesos de IA en lo que llamamos *near realtime*, con la información descargada del sistema embarcado.

NOTA

[4] INS: Inertial Navigation System

Gracias a esta arquitectura, además de aplicaciones para la detección de objetivos y para una navegación avanzada sin dependencias de señal GNSS, también sería posible abordar otro tipo de aplicaciones, manteniendo el mismo enfoque de desarrollo: misiones ISAR avanzadas con realidad aumentada, soluciones para detectar y evitar obstáculos, seguimiento automático de objetivos, *targeting* de precisión, navegación en espacios confinados, enjambres, etc.

Figura 6: flujo funcional para levantamiento de objetivos.
Fuente: expuesto por el autor.

Casos de uso

- **Levantamiento de blancos**

  Se trata de un sistema de inteligencia artificial utilizado para la detección y localización de objetivos, el cual permite reconocer personas, vehículos y animales, así como también el procesado, en tiempo real, a bordo de RPAS y el seguimiento automático de objetivos de interés, por parte del UAV.

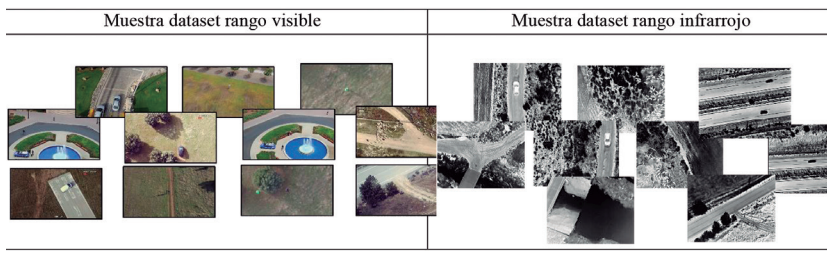


Figura 7: muestra de datasets.
Fuente: expuesto por el autor.

Para ello, se han aplicado técnicas de *deep learning* sobre imágenes aéreas, procesadas en tiempo real con equipos muy limitados, en términos de peso y consumo, para operar a bordo del UAV.

En cuanto al concepto operativo de alto nivel, para alcanzar estas funcionalidades, es imprescindible contar con data sets completos, que permitan

Figura 8: caso real - detección de vehículo..
Fuente: expuesto por el autor.

Figura 9: caso real – detección de personas.
Fuente: expuesto por el autor.

entrenar la red neuronal de acuerdo con las salidas esperadas. En este caso, se está empleando un data set de más de 5800 imágenes, para entrenar la red en la detección de personas, coches y animales, tanto en un rango visible con resolución de 1280 x 720, como infrarrojo, con resolución de 910 x 720.

Gracias a estos bloques de aprendizaje se obtuvo, en una primera ronda, un ratio de éxito para la detección de ensayos en vuelo del 95% para la detección de coches y del 86% para la detección de personas.

Navegación por visión

En este caso, el objetivo es implementar un sistema de navegación avanzada con señal GNSS degradada o denegada, que otorgue la capacidad de posicionamiento global sin señal GNSS, a partir de la información capturada por la cámara y apoyada por el resto de sensores. En ese sentido, podemos mencionar las siguientes funciones:

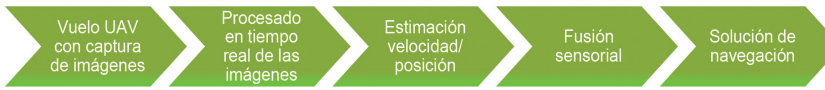


Figura 10: flujo funcional Navegación Avanzada.
Fuente: expuesto por el autor.

- Procesamiento de imágenes mediante inteligencia artificial
- Apoyado en otros sensores embarcados
- Funcionamiento autónomo, a bordo y en tiempo real

Para conseguirlo, se emplea el mismo modelo de implementación que para el caso anterior, pero la aproximación de la solución, al emplear inteligencia artificial es diferente. Desde un punto de vista funcional, la operativa es la siguiente:

- Para obtener una solución de navegación sin señal GNSS es necesario contar con la información de los sensores embarcados (cámara, INS y telémetro). A partir de las imágenes capturadas, se crean dos sensores virtuales: uno que permite la estimación de la velocidad a través del flujo óptico y otro que posibilita el posicionamiento global, identificando patrones, mapeando y referenciando sobre un mapa.

En ambos sensores se emplean redes neuronales que permiten obtener una estimación de velocidad y, por otro

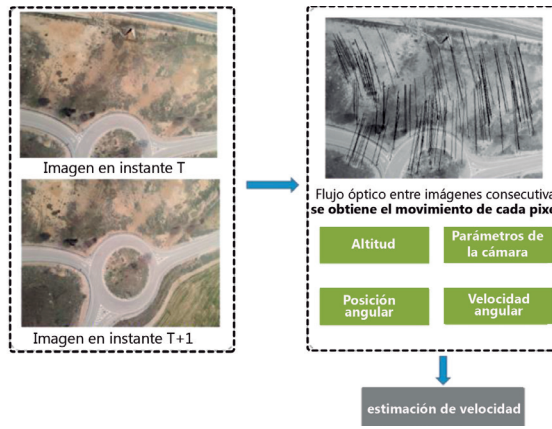


Figura 11: sensor virtual de flujo óptico.
Fuente: expuesto por el autor.

Figura 12: sensor virtual de mapeo de patrones.
Fuente: expuesto por el autor.

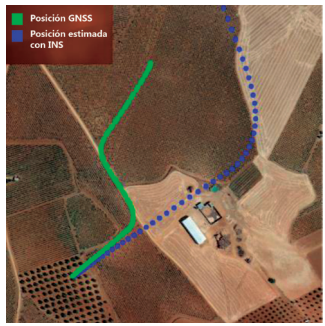


Figura 13: solución GNSS vs solución de navegación inercial.
Fuente: expuesto por el autor.

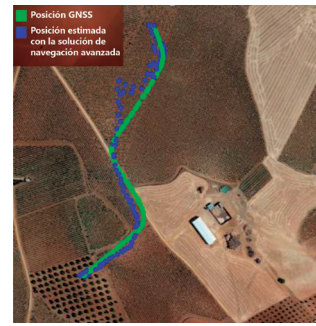


Figura 14: solución GNSS vs solución de navegación avanzada con IA.
Fuente: expuesto por el autor.

lado, alcanzar una solución de posicionamiento global sin necesidad de utilizar una señal de posicionamiento absoluto externa, a través de receptores GNSS.

En estos casos, la inteligencia artificial ha demostrado una gran superioridad ante las técnicas clásicas de visión. Dentro de las principales ventajas sobre las técnicas tradicionales, la visión artificial ofrece mejoras significativas en cuanto a la robustez en los giros de imágenes, independencia del terreno sobrevolado y mejora en tiempos de procesado.

4. Retos para la inteligencia artificial aplicada a los UAVs

Los ejemplos presentados anteriormente son sólo una pequeña muestra del amplio abanico de posibilidades que ofrece esta tecnología. Al final, se trata de sistemas inteligentes con un comportamiento similar al cerebro humano y que, sumados a las capacidades que ya ofrecen los sistemas no tripulados, pueden dotar de ventajas competitivas clave no sólo a los sectores relacionados con la defensa y la seguridad, sino también para cualquier otro sector industrial.

Sin embargo, hay una serie de limitaciones que conviene poner encima de la mesa, ya que no se corresponden únicamente con limitaciones técnicas, sino también con las de carácter ético y moral.

Desde un punto de vista técnico, las limitaciones que aparecen generalmente están asociadas al hardware y a la disponibilidad de modelos de entrenamiento adecuados, algo que supone un reto mayor para esta casuística, debido a que se trata de equipos que deben embarcarse en UAVs, por tanto es importante trabajar en los siguientes puntos:

- Procurar una mayor capacidad de proceso, con pesos y dimensiones cada vez más reducidos.
- Sensores cada vez más precisos y que ofrezcan más información.
- Minimizar el consumo de recursos del equipamiento embarcado.
- Disponibilidad y accesibilidad a *data sets* completos.
- Encontrar soluciones que permitan el escalado, optimización y mantenimiento evolutivo de los modelos de IA en producción
- Facilidad de integración de diferentes soluciones, algoritmos y desarrollos

Cada día aparecen procesadores más potentes, sensores y equipos más pequeños. En cuanto a las bases de datos, poco a poco se están generando data sets cada vez más completos, que permiten entrenar los nuevos desarrollos y validar las soluciones. Por tanto, es sólo cuestión de tiempo disponer de soluciones para las diferentes barreras técnicas que puedan aparecer.

Ahora bien, los retos fundamentales para el desarrollo de la IA no son de carácter técnico. Está claro el beneficio que la IA puede aportar a la sociedad, sin embargo, existe cierto

temor ante la posibilidad de que estos sistemas puedan superar la inteligencia y capacidades humanas; por otro lado, también hay una preocupación generalizada ante el desarrollo, de forma incontrolada, de aplicaciones de IA que puedan representar una amenaza potencial para la humanidad.

Una preocupación inmediata estaría relacionada con el desarrollo de aplicaciones de IA militares, para sistemas letales de armas completamente autónomos (LAWS[5]), algo que quedó ilustrado en un vídeo publicado en 2017 por Stuart Russell, profesor de Ciencia Computacional de la

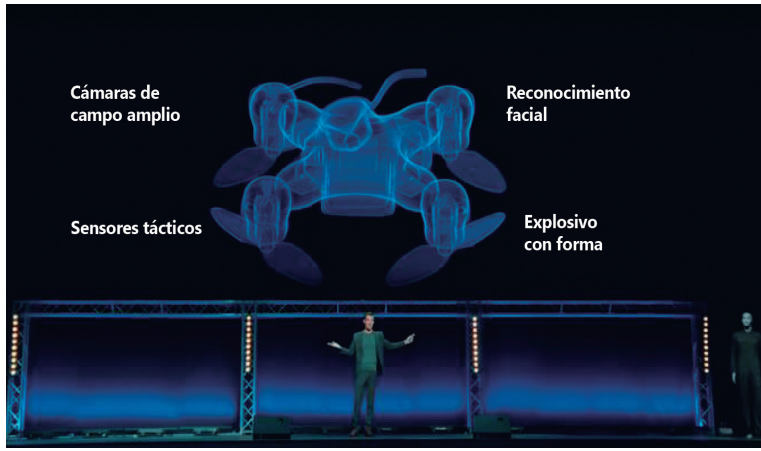


Figura 15: vídeo Prof. Stuart Russell.
Fuente: U.C. Berkeley, 2017.

Universidad de Berkeley y experto en temas de inteligencia artificial. Se trata de un vídeo presentado a delegados de la ONU[6], en la conferencia sobre sistemas autónomos de armas, el cual se hizo viral en pocas semanas. En la grabación simplemente se especuló con la posibilidad de integrar y miniaturizar tecnologías existentes, poniendo en relieve un escenario al que se podría llegar con sistemas LAWS, al operar sin intervención humana.

[5] LAWS: Lethal Autonomous Weapon Systems
[6] ONU: Organización de Naciones Unidas

NOTA

En términos generales, se deben desarrollar y adoptar principios claros para guiar a las personas a construir, usar y aplicar la inteligencia artificial. Estos principios deben considerar implicaciones éticas y sociales, el desarrollo de políticas y una legislación adecuada, implicaciones en términos de privacidad y seguridad, así como los impactos directos e indirectos de los nuevos desarrollos.

5. Conclusiones

Cuando hablamos de inteligencia artificial, nos ubicamos ante una tecnología disruptiva que está transformando todos los sectores industriales y, como no puede ser de otra manera, también los de defensa y seguridad. Además, si combinamos esta tecnología con los UAVs, las posibilidades son enormes; a nadie se le escapa los grandes beneficios que puede ofrecer el desarrollo de esta tecnología a la sociedad, más allá de los conflictos y controversias que puedan aparecer de la mano de esta nueva generación de sistemas y soluciones que habrá que solventar adecuadamente.

Volviendo al plano operativo, hemos visto también dos ejemplos representativos para los que, aplicando esta tecnología, se ha conseguido desarrollar capacidades que eran prácticamente inimaginables hace algunos años y que pueden suponer una ventaja operativa real en el empleo de UAVs. Una de ellas permite transformar un sistema de vigilancia aérea convencional en una solución completa, con mayor conciencia situacional y con la capacidad de detección, clasificación y seguimiento de objetivos de forma totalmente autónoma. Por otro lado, hemos visto también las posibilidades que ofrece la IA para las propias capacidades de navegación autónoma del sistema, permitiendo generar una solución robusta y fiable, con independencia de la señal GNSS recibida.

En definitiva, estamos ante un verdadero catalizador de la nueva revolución industrial, que transformará nuestra sociedad en los próximos años y cuyas posibilidades están en el umbral de nuestra imaginación.

Referencias

Anónimo. Recuperado de youtube.com/watch?v=TIO2gcs1YvM

AI Business (2016) *9 Key AI Ethical Issues & How to Handle Them*.

Arduino. Recuperado de website: www. arduino.cc

Ardupilot website. Recuperado de www. ardupilot.org

Everis Aeroespacial y Defensa S.L.U. (2017) *Robotics and Autonomous Systems in the field of Defence and Security.*

Everis Aeroespacial y Defensa S.L.U. (2018) *Artificial Intelligence and its applications in Aerospace & Defence*.

HPC and AI - *Two communities same future. 2018. HPCwire*

Machine Learning Mastery (2013) *A Tour of Machine Learning Algorithms*.

McKinsey & Company. *An executive´s guide to AI.*

Microsoft (2017) *How to choose algorithms for Microsoft Azure Machine Learning.*

MIT Technology Review (2017). *The Artificial Intelligence Issue*. Vol 120 (6)

MIT Technology Review: The Artificial Intelligence Issue Vol.120 No.6 (November/December 2017)

Kumar, R., Shen, S., Michael, N. & Mohta, K. (2017) *Multi-sensor fusion for robust autonomous flight in indoor and outdoor environments with a rotorcraft micro-aerial vehicle (MAV)*. University of Pennsylvania.

The Hague Centre for Strategic Studies (2017). *Artificial Intelligence and the Future of Defense.*

The Verge (2017). *Robots and AI are going to make social inequality even worse, says new report.*

Time (2016). *This Is the Biggest Battle in Tech Right Now*.

Wharton (2017). *All new electricity*.

SISTEMA DE COMPENSACIONES INDUSTRIALES Y SOCIALES

OFFSET

BLOQUE 5

ANTONIO FONFRIA

ENRIQUE NAVARRO

BLOQUE

5

MODERADOR

EXPOSITORES

SESIÓN 5.1

Calm.
Oscar
Torrico Infantas

Durante este simposio hemos abordado diversos temas de interés y actualidad, que nos hacen reflexionar sobre la importancia de la tecnología, innovación y creatividad en el campo militar, factores indispensables para el desarrollo de nuestros países.

Conocedores de que el presupuesto del sector defensa siempre estará en competencia directa con otras prioridades de nuestros Gobiernos, las compensaciones industriales, o acuerdos offset se convierten en herramientas de suma utilidad para muchos países.

Esta forma de acuerdos, presentes como parte de las estrategias de los países para acceder a la tecnología, ha servido para sociabilizar, en ciertos aspectos, las adquisiciones del sector defensa.

A modo de contextualización, las compensaciones industriales offset se definen como acuerdos comerciales entre el Estado comprador y la empresa extranjera proveedora de bienes, obras y servicios en el ámbito de la defensa, los cuales obligan al proveedor a llevar a cabo, a través de la suscripción de uno o más convenios, proyectos que compensen el flujo de dinero público invertido en la defensa.

Asimismo, el mecanismo offset ha sido empleado por distintos países, desde hace más de medio siglo, como parte de una política de Estado con visión estratégica. Al principio, la orientación de estas compensaciones estaba dirigida hacia el sector militar, sin embargo, en los años 70 se expandió y abarcó a otras áreas del

acontecer nacional productivo.

La posibilidad de obtener beneficios industriales o compensaciones de diversos tipos, ya sea de forma directa en el mismo sector defensa, o indirecta en otras áreas diferentes al campo militar, ha generado oportunidades de acceso tecnológico, incremento de mano de obra capacitada y la reducción de la brecha industrial, con importantes resultados en los niveles de desarrollo industrial en los países que lo implantaron.

A nivel global, podemos resaltar el caso de Canadá que, durante más de 30 años, trató de aprovechar los beneficios económicos más amplios de la contratación de defensa, a través de la Política de Beneficios Industriales y Tecnológicos (ITB) la cual exige que los contratistas emprendan o desarrollen actividades comerciales en Canadá, por un valor similar al contrato del bien o servicio de defensa.

Por otro lado, acuerdos con Lockheed Martin y Boeing han permitido desarrollar actividades en programas de salud, sistemas y software, soluciones de inteligencia artificial (IA), simuladores de aviación civil y tecnología para la industria metal-mecánica.

De acuerdo al informe del Gobierno de Canadá del 2018[1], sobre las políticas de compensaciones y beneficios industriales, entre 1986 a 2017, la cartera global de obligaciones incluyó 144 contratos valorados en 43800 millones de dólares, con 31800 millones de dólares en actividades comerciales ya finalizadas, 8800 millones

NOTA

[1] Industrial and Technological Benefits Policy: Value Proposition Guide, May 31, 2018. Texto completo en: https://www.ic.gc.ca/eic/site/086.nsf/vwapj/VPGuideEng.pdf/$file/VPGuideEng.pdf.

en actividades en curso y 3200 millones de dólares en oportunidades de trabajos futuros no identificados.

Otro caso a resaltar es la experiencia de España, con la adquisición de 72 aviones F-18A a la McDonnell Douglas, en 1983, por 1543 millones de dólares, caso que será meridianamente abordado en los próximos minutos.

En al ámbito regional, Brasil es el país que mejor ha implementado, como una política de Estado, los beneficios ofrecen que los acuerdos offset. Cabe mencionar que dicha nación pasó por una etapa de decisión política en el campo de desarrollo tecnológico y es por ello que, en la década de los 80, impulsó la adquisición militar con miras a recibir una transferencia tecnológica que redujera su dependencia del mercado extranjero[2]. Esta decisión le permitió a Brasil recibir compensaciones en el ámbito aéreo-militar, las cuales se expandieron a la industria aeronáutica brasilera a tal escala que EMBRAER fue, hasta hace poco, el tercer fabricante de aeronaves en el mundo[3], generando no solo puestos de trabajo, sino importantes divisas al Estado brasileño.

En cuanto a la obtención de transferencia tecnológica, fabricación bajo licencia, coproducción y alianzas estratégicas, Brasil logró despegar su industria aeronáutica y con ella otros sectores industriales. Para Vargas[4], los offset en el Brasil jugaron un papel determinante en el

NOTA

[2] FIEGENBAUM, J. y RONDINEL, R. "Acuerdos offset de compensación comercial, industrial y tecnológica: Un estudio del caso brasileño" en Observatorio de la Economía Latinoamericana, Número 68, 2006. Texto completo en http://www.eumed.net/cursecon/ecolat/

[3] VARAMAYO, Pablo A., "Grado de impacto de las políticas de offset-compensaciones industriales, comerciales y sociales en el Cono Sur: Argentina, Brasil, Chile y Perú", Centro de Estudios Avanzados, Universidad Nacional de Córdoba, Maestría en Relaciones Internacionales, pag. 6

[4] VARGAS Vergnaud, Mauricio, "Una Mirada económica a los acuerdos de Offset en el Sector Defensa y Seguridad en Colombia", Departamento Nacional de Planeación, Dirección de Estudios Económicos. Marzo 19 de 2004. Pag. 17.

desarrollo de la industria de defensa, sobre todo en las áreas aeronáutica y naval.

En el caso del Perú, gracias a la vigencia de la "Directiva para normar las adquisiciones y contrataciones de bienes y servicios para la defensa nacional en el mercado extranjero, bajo la modalidad de compensaciones industriales y sociales – Offset", en el año 2011, pudimos recibir los beneficios de estos acuerdos de forma directa.

A la fecha, se han firmado más de 42 convenios específicos. La reciente experiencia obtenida mediante la adquisición de los aviones KT-1 y la posterior implementación de talleres para la coproducción de esta aeronave, la compra de helicópteros MI-171, que permitió la creación del centro de mantenimiento regional de este tipo de naves, así como el relanzamiento de la construcción de nuevas unidades navales (como parte de los beneficios offset) posibilitó la recepción de mejoras en los procesos de la industria naval nacional; por otra parte, permitió no solo incrementar nuestras capacidades industriales, de mantenimiento y producción, sino también nuestra conversión como socio estratégico regional de la fábrica matriz en el caso de los aviones y helicópteros.

En este bloque, recibiremos las ponencias de dos destacados economistas españoles, cuya experiencia profesional y académica se ve sustentada por sus impresionantes biografías. Los doctores Antonio Fonfria y Enrique Navarro, ambos prestigiosos profesionales, abordarán, desde sus propias perspectivas, la importancia de los beneficios del offset y su implicancia en la economía y desarrollo de los países.

Por su parte, el doctor Antonio Fonfria, catedrático de la Universidad Complutense de Madrid, nos presentará, desde la perspectiva de la oferta y demanda, el creciente interés que existe por el volumen de inversión en recursos que se da en el comercio mundial a través de los offset. Asimismo, nos mostrará como los gobiernos pueden obtener un mejor beneficio a través de las compensaciones que se reciben al invertir en defensa, en la medida que se priorice la orientación de esos beneficios. Algunos instrumentos económicos, como las denominadas tablas input-output, nos ayudan a determinar hacia donde deben orientarse las compensaciones industriales, de modo que permitan generar un efecto multiplicador en su desarrollo.

Por otro lado, el doctor Enrique Navarro, fundador y presidente de MQ Globalnet, nos demostrará, a través de diversos casos de éxito, cómo algunos países han obtenido grandes beneficios al implantar adecuadas políticas públicas, relacionadas a los acuerdos offset; también nos presentará los grandes retos que estos acuerdos plantean a las autoridades de un país, toda vez que estas compensaciones, principalmente las indirectas, deben buscar siempre el mayor de beneficio para el tejido industrial, el desarrollo tecnológico, el capital humano y la competitividad. Pero no todo es felicidad en los actuales acuerdos offset, tal como señalará el doctor Navarro, ya que en algunos casos, los proveedores de material militar, al estar obligados a compensar con proyectos que poco o nada guardan relación con sus actividades, generan a su vez cuestiones jurídicas en cuanto a la naturaleza y propiedad de los activos trasferidos, sobre todo de orden práctico.

Finalmente, este bloque cobra especial y relevante interés en la medida en que, en los últimos meses, la institución y el Alto Mando Naval han venido desarrollando e impulsando una propuesta de normativa offset que permitirá establecer las bases para sociabilizar las adquisiciones del sector defensa y, a su vez, atraer la inversión privada para desarrollar diversos proyectos de infraestructura y potenciar el aparato productivo del país.

Recientemente, se aprobó el Plan Nacional de Competitividad, así como el ambicioso Plan de Infraestructura para la Competitividad, presentado hace unas pocas semanas atrás. Esto no hace más que reafirmar el interés por encontrar formas imaginativas e innovadoras para atraer la inversión extranjera.

Por eso es válido hacernos la siguiente pregunta: ¿se puede, de forma simultánea, adquirir activos estratégicos de defensa, reducir las brechas en infraestructura en el país y mejorar la industrialización con el correspondiente incremento de nuestra competitividad? Estoy seguro que esta interrogante será respondida a cabalidad por nuestros expositores, en los próximos minutos.

sesión

5.1

Offsets economía y resultados

Dr.
Antonio Fonfría

El comercio internacional supone uno de los pilares del crecimiento económico. El acceso a los mercados es una condición necesaria para poder explotar las ventajas comerciales, junto a la capacidad de adquisición y absorción en los mercados de destino. En el caso de la defensa, las importaciones de este tipo de material, por parte de algunos países, se ha aprovechado para obtener ciertas capacidades, tanto de las propias adquisiciones de material de defensa, como a través de importaciones e inversiones vinculadas o no a este material, lo cual se ha realizado a través de contratos paralelos a las compras de defensa, en lo que se denominan acuerdos offset.

El presente texto tiene por objetivo profundizar en este tipo de acuerdos y mostrar la utilidad que, para la toma de decisiones sobre el destino de los recursos vinculados a dichos acuerdos, puede tener un instrumento económico concreto: las tablas *Input-Output*.

1. Los offset: concepto, agentes, factores impulsores y conflictos de intereses

Como una forma de contra-comercio, el offset supone un intercambio de bienes y servicios que, en el caso del sector de la defensa[1], se encuentra unido a la adquisición de sistemas de armas por parte del país beneficiario del offset. En este sentido, la compra de esos sistemas suele ir acompañada de diversas contraprestaciones por parte del vendedor, realizadas a través de distintas vías como la coproducción, la transferencia de tecnología o las inversiones directas.

Habitualmente, existe una distinción marcada entre offset directo e indirecto. El primero es aquel que se dirige al producto que lo genera, por ejemplo, si se adquiriesen fragatas, el offset se plasmaría en servicios orientados a ellas, o bien a la misma construcción en el país importador, o bien al sector defensa, lo que podría ser el caso de la creación de un centro de formación avanzada para el mantenimiento de otros sistemas de armas distintos a las

[1] Desde hace algunos años se explora la posibilidad de extenderlo a otros sectores.

NOTA

fragatas. Por otro lado, el segundo requiere que el proveedor compre bienes o realice inversiones que puedan ubicarse en sectores diferentes al de defensa, como alimentación, textil, infraestructuras civiles, entre otros.

El último de un offset recibido por un país es mejorar su situación, en términos económicos, a través de la obtención o generación de nuevas tecnologías, el aprendizaje, las inversiones en diversos activos (fijos o intangibles) y todo tipo de actuaciones en actividades o sectores que consigan un incremento en el desarrollo de capacidades inexistentes, o que se desean impulsar.

En este sentido, es importante destacar la necesidad de considerar diversos aspectos relativos a cuatro ejes fundamentales: las motivaciones para realizar acuerdos offset, las limitaciones que poseen, la selección de los sectores o actividades más adecuadas y la evaluación del impacto económico[2].

Con relación a las motivaciones, al igual que las limitaciones que conducen a la realización de acuerdos offset, eafectan a un amplio conjunto de agentes[3]: los vendedores de los sistemas, los adquirientes y los gobiernos involucrados. En el lado positivo de la balanza, cabría mencionar los factores impulsores de estos acuerdos; obviamente, el beneficio mutuo es la base sobre la cual se asientan, de manera que han de suponer mejoras para los agentes involucrados. Así, desde la perspectiva del exportador, además de los sistemas de armas vendidos, los acuerdos offset permiten penetrar en un mercado que, de otra forma, mostraría mayor complejidad en cuanto a la exportación de bienes o servicios. Igualmente, ofrece la oportunidad de establecer actividades en el largo plazo, evitar problemas relativos a la situación del país adquiriente, respecto a la escasez de la moneda para importar[4], incrementar su cuota de mercado y establecer o ampliar los canales de

NOTA

[2] Este último aspecto se desarrollará en profundidad posteriormente.

[3] Véase Nassimbeni, et. al (2014).

[4] Nótese que el origen de este tipo de acuerdos se encuentra en la dificultad de algunos países para adquirir sistemas de armas y que a través del trueque –barter-, se podían obtener.

distribución de productos, a través del establecimiento de nuevos socios comerciales, y atraer potenciales clientes.

Desde la óptica del importador de sistemas, los acuerdos de compensación brindan habilitación tecnológica, en los casos en los cuales hay transferencia de la misma, así como también reducen la necesidad de divisas para la importación de bienes y servicios, estimulan las curvas de aprendizaje y la absorción de tecnologías, incrementan el contacto con los mercados internacionales — permitiendo la entrada en ellos a través de exportaciones— mejora las capacidades competitivas de las empresas y su productividad, y estimula la entrada de empresas locales hacia nuevos segmentos de negocio o de mercado.

Con relación al tercer agente interviniente, para el Gobierno del país exportador los offset pueden suponer un apalancamiento financiero en sectores importantes. De este modo, si el país se encuentra en vías de desarrollo, las infraestructuras de todo tipo pueden ser objetivos fundamentales para mejorar la cohesión social y territorial de la nación. Adicionalmente, puede mejorar el saldo de la balanza comercial en el mediano y largo plazo a través de un incremento de las exportaciones, como resultado de las mejoras introducidas en las empresas. Junto a ello, la percepción social[5] de las adquisiciones de sistemas de defensa mejoraría sustancialmente, si se aplican offsets indirectos y orientados a sectores distintos a la defensa.

Por otro lado, los gobiernos de los países exportadores experimentarán una mejoría en su balanza comercial, tanto de las exportaciones de material de defensa, como de las subsiguientes exportaciones derivadas de los acuerdos de compensación. Algo similar genera, sobre la balanza financiera, el incremento de las inversiones directas en el país importador, las cuales se mantienen en el mediano plazo.

NOTA

[5] En este caso resulta particularmente importante que el gobierno realice una campaña de comunicación estratégica que permita poner en valor las adquisiciones de defensa como difusoras de la actividad económica global del país.

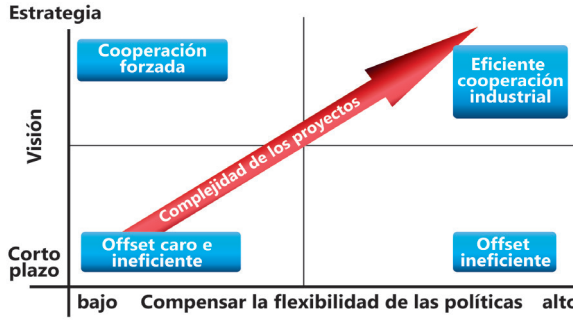


Figura I: factores para una cooperación industrial eficiente.
Fuente: MBDA (2015).

Sin embargo, existen importantes conflictos de interés entre los agentes que participan en los acuerdos, ya que cada uno de ellos posee objetivos diferentes que no necesariamente coinciden. Asimismo, para reducir las fricciones entre los agentes es necesario unir dos factores. El primero de ellos es una visión estratégica y de largo plazo, que permite a los distintos actores cooperar sin esperar resultados en el corto plazo, ya que la propia esencia de los acuerdos offset se encuentra unida a períodos temporales amplios. Esto se aplica en las empresas que intervienen en el proceso, desde la perspectiva importadora, hasta la exportadora e inversora. El segundo factor tiene que ver con la flexibilidad en la aplicación de las políticas offset. En este sentido, la cooperación industrial más eficiente se obtiene a través de políticas innovadoras y creativas, que aporten perspectivas novedosas al proceso de cooperación, a la selección de los sectores y empresas participantes, y a la gestión adecuada de los offsets. Este último aspecto requiere de estructuras de gestión que permitan la aplicación ágil de las políticas y su seguimiento a lo largo del tiempo, así como una evaluación continua, a fin de orientarlas hacia el cumplimiento de los objetivos planteados.

La consideración de los factores mencionados es relevante, debido a la importancia cuantitativa de los acuerdos offset

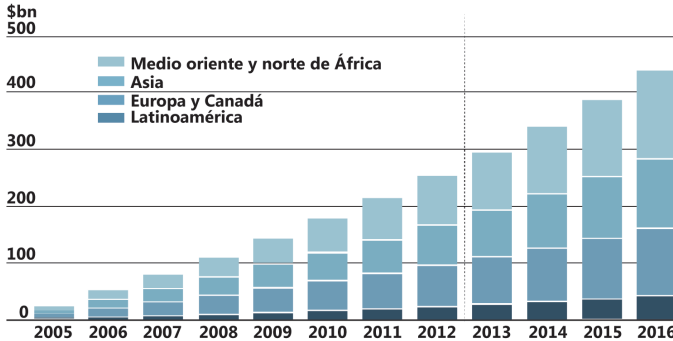


Figura 2: obligaciones de offsets por región.
Fuente: Coates (2015).

y su crecimiento en los últimos años. Como se observa en la figura 2, el crecimiento de las obligaciones unidas a los offsets a nivel mundial es muy importante, ya que alcanzó el medio billón de dólares, lo cual supone el tamaño de economías como la de Suecia o Bélgica. En tal sentido, un volumen que moviliza recursos y genera efectos bastante mayores a esa cuantía (ya que los offsets poseen un efecto multiplicador en la economía) puede cifrarse por encima de 10 veces el valor del offset en algunos casos[6].

2. Las tablas *input-output*, como instrumento de apoyo a la toma de decisiones sobre offsets

Los efectos multiplicadores de los offsets se encuentran en el centro de la elección, en cuanto al tipo de instrumentos a utilizar (financieros, exportaciones, inversiones) y los sectores en los cuales serán aplicados, de modo que se generen los mayores resultados posibles en beneficio de las partes implicadas y, en especial, con relación al país beneficiario de los acuerdos de compensación.

En este sentido, y centrándonos en los offsets indirectos, las prioridades de política económica son las que han de marcar las pautas fundamentales relativas a los factores mencionados.

[6] Véase Vargo (2012) para un análisis de las operaciones financieras de offsets y sus efectos multiplicadores para varios países.

NOTA

Las prioridades sectoriales, regionales y de empleo se encuentran unidas a las perspectivas políticas de los gobiernos de turno, los cuales las desarrollan mediante diversos instrumentos de política económica y social. No obstante, se pueden utilizar instrumentos de apoyo a la toma de decisiones, que aporten una perspectiva más neutra y que arrojen luz sobre las prioridades a considerar, siendo un objetivo básico el mayor incremento del PBI del país, como es el caso de las tablas *input-output* (TIO)[7].

El aumento del producto bruto se puede conseguir de diversas maneras y con distintas distribuciones territoriales, sectoriales, industriales y tecnológicas, por lo que el énfasis en algunos de estos aspectos determina el resultado obtenido y los posibles efectos sobre otros sectores, territorios y tecnologías. Por lo tanto, es importante establecer a priori diversos escenarios sectoriales que permitan anticipar los posibles efectos de la aplicación de los acuerdos de compensación en el país de destino. Por tanto, partiendo del análisis se puede desprender el efecto causado por el aumento de una cierta cuantía económica aplicada a uno o varios sectores, sobre el PBI, el empleo, el valor añadido y el comercio exterior.

Adicionalmente, debido a que algunos sectores poseen una localización territorial concreta y poco extendida por el conjunto del país, se puede aproximar el efecto en términos territoriales, más allá del uso de un análisis geoeconómico ad hoc.

De igual modo, es posible realizar un estudio posterior de los efectos generados por los offsets, utilizando la misma herramienta. La virtualidad de este análisis es que permite conocer los resultados que se plasman en la economía; más aún, a lo largo del tiempo en el que se están aplicando los acuerdos de cooperación, es posible realizar un análisis que sirva de orientación, para mejorar o corregir desviaciones respecto de los objetivos marcados.

NOTA

[7] El desarrollo de las TIO se debe al Premio Nobel de Economía W. Leontief. Un estudio estudio amplio puede verse en Miller y Blair, (2009).

	Sector 1	Sector 2	.....	Sector n	∑.iCI	Consumo	Gasto Público	Inversión	Export.	Demanda final	ET
Sector 1											
Sector 2		Matriz de transacciones interindustriales					Matriz de demandas finales				
.....											
Sector n											
∑.jCI											

R.A.					
E.B.E		Matriz de inputs primarios			
VAB					
IT	X1				

Figura 3: estructura de la tabla input-output.
Fuente: expuesto por el autor.

La figura 3 muestra la estructura general de la TIO.

Por otro lado, en ella se puede distinguir tres grandes matrices. La primera muestra las relaciones entre los distintos sectores de la economía, las relaciones entre ellos, compras y ventas de inputs necesarios para llevar a cabo la producción de cada uno, en lo que se denomina como la matriz de transacciones interindustriales. Por otra parte, la segunda matriz muestra en columnas la remuneración de los asalariados y el excedente bruto de explotación, cuya suma (en ausencia de impuestos) resulta en el valor añadido bruto. Finalmente, los inputs totales configuran la suma de los consumos intermedios y el valor añadido y, por construcción, han de ser iguales a los empleos totales (ET).

La última de las matrices guarda relación con las demandas finales, es decir, incluye tanto el consumo privado, como el gasto público, las inversiones y las exportaciones, es decir, la demanda final de la economía. Sumando esta última columna con la de los ∑.iCI, se obtienen los ET.

En definitiva, aplicando el modelo de demanda a la matriz inversa de Leontief (que no se especifica aquí por sencillez) se puede conocer el efecto de un aumento de la demanda de un determinado sector sobre el conjunto del sistema productivo del país.

Sirva como ejemplo el caso español. A través de las TIO, se calculó el efecto de los offsets en la producción y el empleo. Aunque el análisis es a posteriori, permite ver el efecto generado en términos globales. De esta forma, entre los años 2005 y 2010, los sectores más relevantes en la recepción de offsets han sido electrónica, el sector eléctrico, vehículos a motor, distintos materiales de transporte y otras actividades. El valor medio de sus transacciones en el offset es superior a la media del conjunto y suponen más del 85% de la demanda final generada por los acuerdos de compensación; como puede observarse, son sectores de media y alta tecnología que inciden en los efectos de acumulación y aprendizaje.

Con relación al conjunto de las empresas implicadas, más de 260 son españolas y 180 extranjeras. En este sentido, los offsets intentan estrechar lazos empresariales, aunque no se conoce su alcance y extensión temporal, lo cual requeriría un seguimiento incluso después de terminado el período temporal del acuerdo. Por otra parte, se ha obtenido un efecto total sobre la producción del país, de más de 7700 millones de € en ese período de tiempo, junto con un incremento del volumen de empleo de 9500 trabajadores. Finalmente, es necesario destacar que el efecto multiplicador se encuentra en un factor superior a 3, operación calculada a través del cociente resultante entre el impacto directo generado por el offset y el impacto total que se observa a través de las relaciones interindustriales expuestas en la TIO.

4. Conclusiones

- Los acuerdos de compensación u offsets se muestran como un instrumento de desarrollo industrial que permite mejorar ciertas capacidades de los países beneficiarios. Igualmente, suponen una forma de ampliación del mercado para las empresas exportadoras, incluso brinda la posibilidad de acceder a aquellos con elevadas posibilidades de ingreso.

- No obstante, a fin de obtener los mejores resultados con estos acuerdos, es necesario que exista flexibilidad en cuanto a la normativa reguladora, capacidad de gestión, seguimientos adecuados y trasparencia en las actuaciones que se realicen.
- El punto fundamental para la obtención de los mejores resultados se basa en las prioridades de política económica que se adopten. Éstas pueden orientarse desde diversas perspectivas, como los estímulos a sectores clave, la creación de empleo, el desarrollo de capacidades poco avanzadas en el país tenga, prioridades de tipo territorial, entre otros.
- Para ayudar a la toma de decisiones de este tipo, las TIO se erigen como instrumentos útiles, cuya virtualidad estriba en la posibilidad de realizar simulaciones a priori de los posibles efectos en las principales variables macroeconómicas y sectores industriales, además de la realización de un análisis posterior que permita evaluar los logros alcanzados y las desviaciones, respecto de la situación inicial. En definitiva su utilidad aporta lecciones aprendidas y posibilidades de corrección de cara a otros acuerdos.

Referencias

Coates, K.J. (2015). *Maleficent obligation to marketing opportunity: International success through offset & beyond.* London South Bank University: Working Paper.

MBDA (2015). From Offset to Industrial Cooperation & Offset. Presentado al European Club for Countertrade and Offset Symposium. Recuperado de http://www.ecco-offset.eu/event/symposium-10/

Miller, R.E. & Blair, P.D. (2009) *Input-output analysis : foundations and extensions. Cambridge University Press.*

Nassimbeni, G., Sartor, M. y Orzes, G. (2014) Countertrade: compensatory requests to sell abroad*, Journal for Global Business Advancement.* Vol. 7(1), pp. 69-87.

Vargo, R.J. (2012). Accounting and Financial Reporting for International Trade Offset Obligations. *Journal of Global Business Management*. Vol. 8 (1), pp. 80-85.

sesión

5.1

El Offset indirecto: herramienta de desarrollo económico

Dr.
Enrique
Navarro Gil

En primer lugar, quiero agradecer a la Escuela de Guerra Naval por su amable invitación y por haber decidido introducir la cuestión del offset dentro de la temática de la conferencia. Precisamente, el offset guarda ciertas similitudes con los agujeros negros del universo: todos hablan de ellos, pero nadie sabe muy bien en qué consisten.

Por tanto, previo a introducir la cuestión del offset indirecto, considero imprescindible ofrecer algunas notas definitorias, ya que sin ellas será muy difícil entender lo que explicaré a continuación.

Lo más importante del offset es que se trata de una obligación legal suscrita entre un proveedor de material militar y la nación compradora, la cual tiene una naturaleza accesoria a un contrato principal de suministro. Claramente, estamos ante un contrato sujeto a todas las garantías y condiciones propias de la contratación pública. Su objeto es la generación de actividades económicas corte social o industrial, así como la transferencia de determinados activos, ya sean materiales o inmateriales. De esta manera, la obligación posee un Estado receptor de distintos beneficios y una empresa obligada entregarlos.

Dicha obligación puede adoptar diversos contenidos, clasificándose en función de su asociación al contrato principal, en el caso del offset directo, lo cual implica una compensación relacionada con el suministro principal; por el lado del offset indirecto, la compensación no guarda relación con el suministro. En el primer caso, están incluidas la subcontratación de paquetes de trabajo asociados al contrato principal y la transferencia de tecnología asociada a la producción o mantenimiento de los sistemas o equipos del contrato principal.

En tanto, el offset indirecto posee un marco mucho más amplio, ya que ofrece una compensación independiente del objeto del contrato principal; pero, si el objetivo del

contrato offset está relacionado con la industria militar, en este caso hablaríamos de un offset indirecto militar. En tal sentido, puede fijarse una graduación en la relación, de acuerdo al grado de cercanía con el producto del contrato principal o con la empresa proveedora.

Un offset indirecto militar puede ser la subcontratación de los mismos paquetes de trabajo asociados a un suministro, para una entrega similar a un tercer cliente. Por ejemplo, si una empresa nacional recibe una subcontratación para fabricar equipos electromecánicos del suministro principal y la empresa que asume la obligación del offset frente al Estado subcontrata esos mismos paquetes de trabajo para otros clientes, este sería un tipo de offset ajeno al contrato principal.

En casos extremos, podríamos encontrar compensaciones que no guardan relación alguna con el suministro, ni siquiera con el cliente, hecho que normalmente ocurre en los ministerios de defensa. En muchas ocasiones, los países (especialmente las naciones en vías de desarrollo) optan por dirigir el offset hacia actividades civiles, en función de las prioridades nacionales; asimismo, podemos encontrar una amplia gama de actividades potenciales, las cuales se clasifican en inversiones, transferencia tecnológica, adquisiciones, educación y equipamiento de infraestructura en su más amplio contenido.

Pueden existir diversas razones por las que el offset indirecto adquiera una naturaleza prioritaria para un país. En algunos casos se debe a la ausencia de una industria militar, con capacidad para producir o mantener los equipos adquiridos; en otros, la causa debe buscarse en las necesidades o prioridades de cada país y, finalmente, para generar a la sociedad un retorno más allá del que pueden encontrar con la seguridad que conlleva la adquisición militar.

Todos somos conscientes de que las inversiones militares presentan grandes dificultades de entendimiento por el

conjunto de la sociedad, que visualiza otras prioridades en cuanto al destino de los recursos públicos. En el campo de la defensa y la seguridad, es muy difícil desarrollar una percepción social de inseguridad, respecto a las compras militares; a menudo, cuando esto se produce, es demasiado tarde. Muchos países han utilizado el offset como un mecanismo para justificar inversiones militares y, sobre todo, para contribuir al desarrollo económico, industrial y tecnológico de una nación.

Si analizamos la evolución histórica de los países que han venido desarrollando políticas offset en las últimas décadas, notaremos una tendencia natural desde la preeminencia del offset indirecto, hasta una aparente concentración de las prioridades en el offset directo. Las razones son variadas, pero sin duda, la principal es la creciente necesidad de garantizar el soporte a los sistemas adquiridos.

Todos somos conscientes de que el mantenimiento de un sistema genera un coste a las arcas públicas, que muchas veces excede del valor de compra y, en algunos casos, incluso la duplica. La escasez presupuestaria para la defensa, en muchos países desarrollados, ha llevado a este proceso de transferencia del offset desde la óptica indirecta hacia la directa.

En la actualidad, muchos países europeos y emergentes (como Turquía, Corea o Singapur) están reclamando una participación con contenido local ; de esta manera, los gobiernos están impulsando a las empresas para que alcancen acuerdos de coproducción o subcontratación con empresas locales. Sin embargo, este tipo de acuerdos exige una total confianza de las fuerzas armadas en la industria local, para asegurar que no se produzcan alteraciones o problemas en la ejecución del contrato principal. Además, este tipo de acuerdos dificulta mucho la aplicación de penalidades por incumplimiento, ya que nos encontraríamos con problemas mayores en la propia ejecución del contrato principal.

Por otro lado, el offset indirecto presenta significativos inconvenientes para las partes afectadas. En cuanto a las fuerzas armadas y agencias de offset militares, les obliga a tratar con un contenido desconocido y para el cual se necesitaría un gran conocimiento de la economía y la industria civil; en el caso del obligor, presenta un doble problema: debe buscar a un sponsor o a una tercera persona que tenga el conocimiento, el producto o la necesidad, para cumplir con ese offset y, además, tendrá que pagar por ello. Mientras el offset permanezca en el ámbito de las capacidades del obligor, este tendrá un coste interno, lo cual no implica un cash out. En el supuesto escenario en el que se deba pagar a un tercero, esto impactará sobre la cuenta de resultados del programa.

Teniendo en cuenta estas circunstancias, también hay que decir que el offset indirecto abre un abanico de oportunidades. Su principal beneficio es que permite adquirir determinados activos o capacidades ausentes en el mercado. Es decir, por muchos recursos que se tengan, nadie está dispuesto a venderlas (pues muchas veces estas capacidades no se encuentran en el mercado).

A su vez, el offset indirecto plantea una interesante cuestión sobre la naturaleza jurídica del mismo, ya que, siendo su naturaleza la de un contrato asociado a uno principal, el hecho de que intervengan terceras partes, ajenas al contrato principal o a la cadena de suministro, y que su objeto difiera totalmente del contrato central, hace que cuestionemos su naturaleza de contrato accesorio.

Sin embargo, debemos insistir en este último punto, debido a que el contrato offset tiene una vida que depende del contrato principal y porque comparten la misma causa, la cual constituye un elemento esencial en cualquier contrato.

En los últimos años, los grandes importadores de sistemas de armas han regresado al empleo del offset civil, relacionado con la complejidad de los sistemas que

se adquieren. Es evidente que la tecnología de los países más desarrollados avanza mucho más deprisa que la capacidad industrial de las naciones en desarrollo; de esta manera, para los países del Medio Oriente (que en ocasiones adquieren cazas de última generación) pensar en comprar determinadas capacidades industriales relacionadas con el software resultaría imposible, dada la carencia del conocimiento al interior del país.

De esta manera, muchas naciones están generando grandes proyectos offset para implementar sus principales adquisiciones, de modo que resulten emblemáticas y generen suficientes externalidades para la asignación de fuertes multiplicadores, lo que configura el principal incentivo que tienen las empresas para apostar por un offset de mayor calidad.

En definitiva, y para terminar con esta introducción, debemos poner en valor las capacidades que el offset indirecto puede generar en los países, aunado al hecho de la justificación política y social de determinadas inversiones asociadas a los beneficios del offset.

Uno de los principales retos a los que deben enfrentarse las agencias offset, en el campo civil, es la valoración de las actividades elegibles. En los casos de las subcontrataciones y la compensación directa, resulta sencillo, ya que se dispone de información muy refinada respecto al contrato principal y su contenido; pero, cuando se trata de abordar una apertura de mercados, o una inversión en infraestructura, o en educación, existen carencias de información que dificultan, sin duda, la determinación del valor del offset, lo que sin duda es el corazón de toda la gestión de las compensaciones.

En tanto, aplicar criterios de valoración de costes y multiplicadores es muy complejo, ya que resultará imposible conocer cuáles son los costes reales de cada transacción, debido a que no existe información en el

mercado y a la generación de una situación no balanceada en el tratamiento y disposición de la información. Ante estos desequilibrios, resulta mucho más aconsejable acudir a mecanismos de valoración del output generado, lo que normalmente resulta mucho más evidente para los organismos competentes de la gestión del offset.

Una vez introducida la cuestión del offset indirecto, quisiera centrarme en el aspecto práctico de la cuestión, complementando la excelente presentación del profesor Fonfría. Mi objetivo es presentarles diversos casos de éxito de offset indirecto, cada uno de los cuales engloba una categoría diferente de este tipo de compensación.

En ese sentido, encontraremos casos que se centran en la generación de nuevos mercados, en las exportaciones, en inversiones en infraestructuras y educación, en actividades productivas, o en procesos de transferencia de tecnología, que pueden englobar fórmulas muy diferentes que van desde la pura formación, programas de becarios, procesos on the job training, programas de equipamiento educativo, entre otros. Cada uno de estos casos reales nos permitirá entender mejor la casuística y el nivel de complejidad de su gestión.

Apertura de mercados

Hasta el periodo de industrialización de la guerra, a finales del siglo XIX, casi todos los países fabricaban sus propias armas y barcos. No había electrónica, ni comunicaciones, ni sistemas sofisticados, sin embargo, el tremendo avance tecnológico de algunas potencias implicó, para la mayoría de los países, la adquisición de sus sistemas de defensa en el exterior.

Eran tiempos en los que la defensa consumía más de una cuarta parte de los presupuestos públicos, de manera que estas importaciones significaban una dedicación de reservas de oro o divisas que no estaban al alcance de la mayoría de naciones. Asimismo, eran épocas en los

que el escaso comercio internacional se producía entre las colonias y la metrópoli. Así nació el offset: los países vendedores debían adquirir productos y materias primas de otras naciones, para que estos obtuviesen las divisas con que pagar sus importaciones de armamento.

De hecho, la apertura de la gran mayoría de mercados de exportación, en el primer cuarto del siglo XX, fue gracias a los acuerdos offset. Hoy en día, muchos países ven en los acuerdos de compensaciones un instrumento para acceder a los complejos mercados de Norteamérica y la Unión Europea. De hecho, alrededor del cincuenta por ciento de los acuerdos offset están ligados a convenios de exportación firmados con los países suministradores de los sistemas de armas.

Por otro lado, mediante los acuerdos de Barter, los países exportadores conseguían diversos objetivos, más allá del hecho de contribuir a sus exportaciones; de este modo, se obtenían materias primas y productos agrícolas a precios muy competitivos y, además, generaban una dependencia económica que terminaba siendo política, hecho especialmente significativo en extremo oriente y en Latinoamérica. Por lo general, la competencia entre los potenciales países suministradores terminaba se centraba en el aspecto de la compensación, más que en el propio suministro.

Desde el punto de vista de la eficiencia, este tipo de transacciones presentan problemas añadidos; el principal es el alto índice de fracasos que se producen y existen diversas razones que lo explican. A menudo, los suministradores no disponen de las relaciones necesarias dentro de sus países, para forzar acuerdos comerciales; otras veces, las empresas de los países compradores no reúnen los requerimientos de calidad y de seguridad que demandan los países importadores.

En consecuencia, más del 70% de los intentos por cerrar transacciones de este tipo fracasan, a pesar de generar una voluminosa carga de trabajo.

En lo personal, considero que debemos centrar las actividades de exportación en productos o servicios que cumplan con los requerimientos del comprador y que éste sea forme parte de la cadena de suministro del vendedor. Esto facilita, sin duda, la generación de un acuerdo satisfactorio para todas las partes.

Pero también debo añadir, que, en los numerosos casos de éxito producidos, se han alcanzado factores de multiplicación muy altos, en algunos casos superiores al 50%. De hecho, es muy habitual que las empresas locales, que pasan a formar parte de la cadena de suministro de las grandes corporaciones, continúen en esta labor una vez terminada la obligación, gracias al entrenamiento recibido y a la calidad del producto o servicio entregado.

Una primera experiencia en España, con un proyecto de offset asociado a un programa de exportaciones, se produjo con el contrato de compensaciones asociado a la adquisición de aviones de McDonell Douglas, que fueron destinados a la Armada Española. El objetivo preestablecido para este acuerdo era generar un offset indirecto equivalente al 50% de la obligación.

Después de decenas de reuniones con asociaciones empresariales, para conocer cuáles eran sus inquietudes y prioridades, detectamos que determinados productos hortofrutícolas y del sector de automoción español, muy competitivos en mercados europeos y asiáticos, apenas tenían entrada en Estados Unidos. Las razones eran más culturales que legales: desconocimiento de las normas del mercado, determinación de potenciales importadores, entre otras muchas.

En ese sentido, consideramos que, al tratarse además de un proyecto FMS, el Gobierno de Estados Unidos apoyaría

proyectos de offset que cayeran bajo su área de influencia; de esta manera, concluimos que las Fuerzas Armadas Norteamericanas, uno de los mayores consumidores unitarios de Estados, eran una excelente oportunidad.

Se analizaron más de 130 casos de transacciones potenciales de exportaciones, incluso aquellas que fracasaron, pues pueden extraerse lecciones muy positivas. Por ejemplo, para la exportación de productos de la huerta, como el pepino o el calabacín, resultaba necesario modificar más de 22 características propias de nuestros productos, para adaptarlas a los requerimientos propios del ejército norteamericano.

Sin embargo, las pequeñas empresas familiares españolas no estaban preparadas para acometer las inversiones y cambios necesarios, por lo que finalmente optaron por renunciar a esta vía. En la actualidad, Estados Unidos sigue siendo un mercado muy minoritario para este tipo de productos.

En el lado positivo de la balanza podemos indicar que, gracias a este acuerdo offset, se consiguió realizar el primer FMS inverso. El Ministerio de Defensa de España suministró, a las Fuerzas Armadas Norteamericanas, vehículos de seguridad fabricados en España para las Fuerzas Armadas Españolas. De esta manera, las fuerzas estadounidenses estacionadas en Europa adquirieron vehículos en las ventajosas condiciones ofertadas al Gobierno de España.

El precio total de la transacción ascendió a más de diez millones de dólares, pero debo añadir que el efecto multiplicador de esta compra fue enorme, ya que no solo el mantenimiento de los vehículos sería contratado en España, sino que continuaron adquiriéndose de forma directa, consiguiendo un doble objetivo: mejorar el acceso al mercado y, obviamente, alcanzar ventas que permitieron cerrar una transacción muy voluminosa y satisfactoria.

La principal lección que debemos extraer de este proyecto es la necesidad de mantener una estrecha relación con los productores y exportadores, para conocer sus necesidades y definir cuáles son las mejores líneas de acción. Por tanto, resulta esencial realizar presentaciones públicas sobre el offset y las oportunidades que presenta para los agentes económicos del país, generándose además una expectativa positiva sobre el desarrollo de la política de offset en el país.

En este proyecto, además, se consiguieron otros importantes hitos relacionados con la apertura de mercados, aunque se tratara bajo la categoría del offset directo. Gracias a la capacidad de la industria nacional en el campo de la simulación acreditada, especialmente en el programa F-18, Estados Unidos decidió adquirir, de manos de una empresa española, los simuladores del AV8-B para el cuerpo de Marines de Estados Unidos. De este modo, Estados Unidos no solo se consiguió un suministro de altísimo nivel tecnológico, sino lo que es más importante: una empresa española se instaló en Estados Unidos y que, después de treinta años, continúa siendo un proveedor habitual de equipos de simulación y de mantenimiento para las Fuerzas Armadas de dicho país.

Un segundo tipo de proyectos en el ámbito del offset civil está relacionado con los proyectos de infraestructuras y, en particular, con la generación de inversiones para satisfacer las necesidades del país adquirente, especialmente en naciones en vías de desarrollo, que encuentran dificultades para financiar sus proyectos. Para que estos proyectos sean eficientes, desde el punto de vista de su impacto, resulta imprescindible acumular una masa crítica bajo la óptica del importante valor del offset y, obviamente, concentrar dicho valor en un único proyecto emblemático

Asimismo, para que un proyecto offset de esta naturaleza sea factible, se requieren tres factores:

- Decisión política

  Asignar el offset a un gran proyecto de inversión, para satisfacer una necesidad de envergadura, solo será posible en la medida que se genere un gran acuerdo político, con el objetivo de minimizar los riesgos derivados de las críticas al proyecto, que puedan ralentizar el proceso de la compra principal.

- Selección adecuada del tipo de proyecto

  Se sobreentiende que el offset no financiará un proyecto de infraestructura, lo que quiere decir que la necesidad debe ser previa y lo que se pretende solventar con el offset representan los obstáculos que lo hacen inviable. Este es el caso de los contratos de inversión asociados a acuerdos de concesión o de explotación, o acciones como mejorar la TIR del negocio para atraer a inversores, reducir el coste de la financiación con una subvención de tipos de interés, cubrir con el offset las necesidades de tecnología, ingeniería o actividades de contenido específico, para las cuales es necesario contar con socios extranjeros.

- Disponer de un proyecto emblemático

  Un offset de esta naturaleza no puede ser la suma de diferentes transacciones o acuerdos; es necesario contar con un gran proyecto de adquisición, normalmente asociado a plataformas navales o aéreas, únicos casos de proyectos que pueden generar un valor sustancial.

En general, estos tipos de proyectos son muy escasos y se han producido especialmente en países africanos y en Europa, durante los años cincuenta, para la financiación de inversiones necesarias no solo para el desarrollo económico del país, sino también por razones estratégicas.

Como proyecto de inversión, debemos ubicar un caso de offset civil asociado a unas concesiones mineras en un país africano. En este caso se solicitó a la empresa concesionaria la construcción de un terminal portuario de carga de material a granel, para dar salida a numerosos productos agrarios y materias primas producidos en el país adquirente.

El modelo fue el de una inversión privada asociada a la concesión de la explotación del terminal, por treinta años prorrogables. En tanto, la inversión estimada fue de 36 millones de dólares, en 1982, y el valor estimado del offset alcanzó los 3,5 millones de dólares.

Esto significa que, con un crédito de offset equivalente al 10% de la inversión, se apalancó un proyecto de gran envergadura que, en la actualidad y bajo su nueva prórroga, ha requerido nuevas inversiones. Dicho sea de paso, este proyecto ha generado más de mil empleos directos y una contribución al PIB del país equivalente al 1%.

Como citaba anteriormente, en Europa, mediante los acuerdos offset asociados a compras bajo el modelo FMS, se financiaron las construcciones de ciertas infraestructuras como aeropuertos, oleoductos, redes eléctricas y diversos sistemas de comunicaciones que, más allá de sus implicaciones estratégicas, generaron capacidades muy adelantadas a su época en los países del sur de Europa.

El éxito de estos proyectos se asegura a través de la concurrencia de dos factores. Uno de ellos es la negociación del offset, en paralelo a la adquisición del sistema principal. Seguramente será mucho más complicado encontrar a un buen sponsor del proyecto que, a un proveedor del sistema de armas. Muchos potenciales proveedores de equipos no se sentirán cómodos bajo este paraguas, así que debe procederse de forma simultánea en esta negociación; el segundo factor que debemos considerar es que, antes

de presentar el proyecto, tendrá que realizarse toda la ingeniería del proyecto, con los análisis respectivos de coste y beneficio, así como la disipación de las incertidumbres asociadas al lanzamiento del proyecto, punto esencial para que el mismo sea tomado en cuenta por los potenciales obligors. De esta manera, es recomendable no solo haber identificado el proyecto elegible, sino disponer de todos los costes y ventajas del proyecto, con el mayor grado de detalle, de tal manera que se permita a los proveedores buscar a los sponsors más adecuados para cada proyecto.

Si deseamos que estos proyectos resulten positivos, necesitan de una inversión privada y ser explotados en asociación con una cuenta de resultados. De esta manera, un solo proyecto puede generar infraestructura única, que a mi juicio debería asociarse a algún proceso productivo, de modo que resulte más atractiva para todas las partes.

Otra categoría de proyectos, la cual es muy atractiva para los gobiernos y empresas proveedoras, es la relacionada con los proyectos educativos. Para los compradores, asignar recursos offset al sector educación produce un impacto social muy positivo y un efecto multiplicador enorme a largo plazo.

Para los proveedores, este tipo de proyectos encaja con sus políticas de responsabilidad social corporativa, apoyo a proyectos de desarrollo y a la infancia. En tal sentido, es bastante habitual encontrar iniciativas de esta naturaleza, en casi todos los países que han desarrollado o ejecutan políticas de offset.

No se trata de una categoría muy uniforme, sino que, bajo este tipo de proyectos pueden darse innumerables tipos de actividades. Quisiera citar, en este sentido, dos ejemplos que pueden ilustrar la casuística de estos proyectos.

El primer caso es la creación de una universidad orientada para las empresas, con especialidades asociadas a la

ingeniería y escuela de negocios. Para el país, representaba una necesidad buscada hacía décadas; las necesidades de este tipo de personal se cubrían enviando a personal al extranjero, o bien importando mano de obra cualificada.

El Gobierno tenía clara la necesidad y disponía de los recursos necesarios para la construcción de la infraestructura, pero ésta fue la parte menos complicada del proyecto. Lo importante fue conseguir la acreditación de escuelas de negocio avanzadas a nivel mundial que validasen el proyecto, que aportaran profesores y metodologías de trabajo, material para laboratorios, programas de becas y de formación on the job training, para los estudiantes. El coste de obtener todas estas capacidades directamente, en caso fuera factible, resultaría muy oneroso; por tanto, este emblemático proyecto offset permitió cubrir las carencias principales que presentaba la universidad.

Hoy en día la universidad es una realidad, con más de cinco mil estudiantes y un cuerpo de 200 profesores e instalaciones modélicas. Lo más resaltante es que la generación de este proyecto ha servido para crear un polo intelectual del que se carecía en el país. La interacción empresa - universidad constituye, sin duda, el principal atractivo del proyecto lo ha convertido no solo en un referente nacional, sino que alumnos de la región acuden a formarse en esta institución de referencia.

Sin embargo, son muy escasos los proyectos que adquieren esta envergadura educativa, ya que sólo grandes adquisiciones permiten apalancar un proyecto como éste, el cual consumió cientos de millones de créditos de offset.

A modo de ejemplo, puedo citar proyectos de e-learning para zonas remotas o de difícil acceso, que han permitido proyectos de alfabetización con una escasa infraestructura y el apoyo de centenares de profesores formados bajo el paraguas del proyecto offset. En otros casos, se generó la entrega de material educativo como iPads y ordenadores

para mejorar los medios educativos en determinadas zonas. Sin embargo, también existen numerosos programas educativos exitosos, como son los programas de becas y de formación on the job training.

La mayoría de las grandes corporaciones de defensa disponen de instituciones educativas de prestigio, por lo que les resulta muy fácil organizar programas de becarios que permitan a jóvenes preparados realizar estudios de posgrado o de perfeccionamiento en centros de calidad. En estos casos, es habitual que los países compradores, que aceptan este tipo de transacciones, impongan a los estudiantes unas condiciones de retorno al país, para asegurar la existencia de un beneficio nacional, más allá del que recibirán los propios estudiantes.

Pero más importantes todavía son los programas de formación en las empresas, ya que permiten a profesionales de diversas ramas perfeccionar sus conocimientos, trabajando en grandes corporaciones industriales, en actividades que pueden ir desde procesos sencillos de fabricación hasta laboratorios de investigación y desarrollo.

Para los obligors, este tipo de proyecto resulta muy atractivo, ya que se trata de costes internos; no necesitan pagar a terceros por dicho servicio, sino solo convencer a sus departamentos de recursos humanos de las ventajas de este tipo de proyectos. Normalmente, estas iniciativas exigen a los países compradores que cubran los gastos de viaje o estancia, debido a que financiar actividades de escaso valor añadido con offset, resulta extremadamente caro y reduciría, de forma considerable, el retorno del valor del offset.

A través de estos ejemplos, he explicado modelos de trabajo basados en el offset indirecto, con el propósito fundamental de comprender los mecanismos que pueden desencadenar el éxito o fracaso de este tipo de proyectos. Como han podido observar, las posibilidades son amplias

y es muy probable que muchas de las necesidades de cada país sean satisfechas con proyectos offset; por otra parte, intenté demostrarles que el offset indirecto continúa siendo una prioridad en numerosos países, especialmente en los que se encuentran en vías de desarrollo. Estoy seguro que estas naciones maximizarán el valor del offset de manera mucho más eficiente, invirtiendo en proyectos civiles.

La determinación de las prioridades corresponde a cada país, en función de su idiosincrasia y necesidades. Cada uno deberá desarrollar su propio modelo de acuerdo a sus necesidades, pero debemos admitir que, en la actualidad, la demanda de offset civil es creciente y cada vez más sofisticada, por lo que las empresas están mejorando sus capacidades internas para atenderlas.

No quisiera finalizar mi ponencia sin traer algunas de estas reflexiones al caso del Perú. Ustedes comenzaron a desarrollar su política de offset hace años y he de decir que lo hicieron de forma exitosa. De cara a la nueva legislación que se prepara, para adaptar la política a las nuevas necesidades, resultará fundamental establecer líneas de acción claras, que determinen, tanto a los potenciales suministradores, como a los beneficiarios, la manera en la que deberán conducir sus negocios con respecto a este tema; como explicaba, la difusión de la política offset al interior del país y en los foros internacionales constituye, sin duda, un objetivo prioritario para que esta nueva fase sea exitosa también.

Asimismo, los proyectos emblemáticos ofrecen una ventaja considerable para asentar una política de offset; así lo hicieron la gran mayoría de los países, ya que son tantos los beneficios que pueden derivarse, en cuanto a la generación de confianza; proyectos que, por encima de todo, deben ser sostenibles financieramente y en el tiempo, para que de esta manera extiendan todas sus ventajas.

Ustedes cuentan con la tremenda experiencia del Comandante General, miembro del comité de expertos de la Global Offset and CounterTrade Association, y asiduo conferenciante en numerosas sesiones; por otro lado, también cuentan con una estructura ministerial adecuada para manejar el offset de manera eficiente. Sin duda, son muchas las necesidades que el offset podría cubrir y les animo a que continúen en esta tarea, que no hará más que traer más beneficios para su país.

PALABRAS de CIERRE

Contralmirante
Jorge Andaluz Echevarría
Director de la Escuela Superior de Guerra Naval

Señor Almirante Fernando Cerdán Ruiz, Comandante General de la Marina, damas y caballeros que nos acompañan hoy.

Después de dos jornadas y media, habiendo escuchado las ponencias de nuestros expositores, nos queda un sentimiento de satisfacción, primero por haber corroborado los antecedentes que les precedían en cuanto al prestigio, calidad y profundo conocimiento en los temas que trataron; en segundo lugar por el interés generado en los asistentes, materializado muchas veces en preguntas muy oportunas que permitieron profundizar aún más los tópicos programados y, en tercer lugar, por el vínculo generado entre expositores, moderadores y asistentes.

El solo hecho de conocernos no solo contribuye a fortalecer las relaciones entre nuestras Armadas y naciones, sino que permiten entablar lazos de amistad que perduran en el tiempo y, por último, tenemos la sensación de haber estado a la altura de las expectativas que la Marina de Guerra del Perú tuvo sobre el V Simposio Internacional de Seguridad y Defensa.

En este momento resulta oportuno reconocer y agradecer a las personas, instituciones y organizaciones que posibilitaron la realización de este evento. A la Marina de Brasil, a la Marina de los Estados Unidos de América y a la Armada Española nuestro agradecimiento, por habernos permitido contar con Oficiales de alta graduación, los cuales tuvieron que hacer un alto en sus importantes responsabilidades para estar con nosotros como expositores. A todas las Armadas que se hicieron presentes con sus representantes, a la Naval War College, nuestro agradecimiento una vez más por la importante presencia de sus profesores, a todas las empresas y al Tecnológico de Monterrey, que con sus más importantes especialistas nos ilustraron sobre diversos tópicos tecnológicos. A los especialistas en offset que nos visitaron desde España, a la importante participación de nuestros moderadores, a la

Comandancia General de la Marina, a la Dirección General de Educación por el apoyo permanente que tuvimos para la realización de este Simposio y finalmente, al equipo de trabajo de la Escuela Superior de Guerra Naval, que desde el primer día del año trabajaron con la mayor voluntad posible durante su planificación, coordinación y ejecución.

No quiero terminar mis palabras sin antes comentarles que el VI Simposio Internacional de Seguridad y Defensa SISEDE se llevará a cabo el 2021, año en el que nuestra Marina de Guerra, que encarna el poder naval del Perú, cumple 200 años de existencia. Por lo tanto, resultará oportuno centrar el tema en el poder naval, para lo cual esperamos contar con autoridades navales de las Armadas amigas, para tomar conocimiento de primera mano sobre la visualización del uso del poderío naval en el futuro.

Nuevamente, muchas gracias. Les deseo a nuestros amigos que han venido de otras partes del mundo un feliz retorno y los esperamos para el VI SISEDE 2021.

V SIMPOSIO INTERNACIONAL

DE SEGURIDAD Y DEFENSA

PERÚ 2019

Tecnología, innovación y creatividad en el campo militar

PALABRAS de CLAUSURA

Almirante
Fernando Cerdán Ruiz
Comandante General de la Marina

Damas y caballeros, tengan ustedes muy buenos días. Antes de clausurar este evento, quisiera hacer una reflexión sobre este último punto del offset. En el año 2009, durante mi estancia en el Ministerio de Defensa, tuve la oportunidad de proponer el desarrollo e implementación de la Política Nacional de Offset, para el sector de las Fuerzas Armadas, la cual fue autorizada por el entonces ministro Antero Flores-Aráoz. Posteriormente, en el año 2010, fue culminada con el Ingeniero Rafael Rey; para poder entender qué era el offset, lo primero que se decidió fue viajar a los congresos internacionales de la *Global Offset and Countertrade Association*, ya que no existen universidades, libros o foros de offset en el mundo.

En realidad, es una comunidad cerrada. Acá tenemos a dos miembros de esa comunidad, quienes tuvieron la gentileza de visitarnos y que, realmente, viven de ese conocimiento. Precisamente, el lugar adecuado para entender qué es el offset es en estás convenciones mundiales, donde uno queda encerrado en un hotel durante tres días, desayuna, almuerza y cena los temas vinculados al offset. Es ahí cuando uno empieza a entenderlo y, de regreso al Perú, es posible explicar estos temas, sin embargo, pocos son los que terminan convencidos de las políticas offset. Por eso, a veces es mejor traer extranjeros, ya que, además de entenderlos, les van a creer. Por ello fue que los invitamos y agradezco a estos expositores por compartir sus experiencias con nosotros.

El offset es un mecanismo hecho por las empresas de defensa para vender más. Aquí los llamamos compensaciones industriales y sociales, pero no nos engañemos: este es un mecanismo que elaboran las empresas para aumentar sus ventas y rentabilizar políticamente las compras del sector defensa de un país. Entonces se preguntarán, ¿dónde está el aporte social? En los puestos de trabajo y en los impuestos que se puedan generar a través de un offset bien elaborado. En una

oportunidad, alguien del Ministerio de Defensa me dijo que no veía, en el área legal, la rentabilidad social del offset y en realidad, después de explicarme su visión sobre el offset (que era bastante negativa) le pregunté qué opinaba sobre el offset compuesto y esta persona me dijo que no podía opinar sobre eso, porque no conocía el tema. Entonces, le dije que estaba opinando sobre un tipo de offset que tampoco conocía, ya que no existe el offset compuesto y, cómo él lo explicó, no fue la forma correcta.

Por eso es importante entender este mecanismo, el cual ofrece múltiples posibilidades. El Perú ha invertido, en los últimos dos años, dos mil millones de dólares en compras con offset. Ya se mencionaron algunos ejemplos en la Fuerza Aérea, en el Ejercito y también en la Marina, por lo que añadiré que lo invertido representa, según el Centro de Estudios Económicos de la Sociedad Nacional de Industrias, un 0.96% del PBI, pero lo redondearemos en un punto.

Precisamente, el retorno del Offset recayó en las Fuerzas Armadas. Sin embargo, también pudo haber ido a otros rubros y generar incrementos en el PBI, colaborando así con el desarrollo nacional. De hecho, la primera vez que viajé a este congreso mundial de offset en el extranjero, acudí a la Sociedad Nacional de Industrias, en el año 2009, para hacer una exposición y, posteriormente, viajé con el presidente de la institución a estos eventos. En otra oportunidad, junto al expresidente de la SNI Luis Salazar Steiger, viajamos a otro congreso, en el que los industriales obtuvieron una visión empresarial distinta, respecto a cuáles eran los beneficios que se podían obtener del offset.

En tanto, tenemos diez años con esta política y hemos venido trabajando con el offset directo y, como bien dijo el doctor Navarro, es lo que nos permite mantener el ciclo de vida del producto, a través de las diversas etapas del mantenimiento. Sin embargo, estamos por pasar al offset

indirecto. En ese sentido, le hicimos una exposición al ministro de Economía, hace unos meses, sobre la necesidad de tener una Ley de offset indirecto, para beneficio de otros sectores del Estado. Todos quisiéramos tener unas Fuerzas Armadas del primer mundo, pero para ello debemos ser un país desarrollado y el Perú tiene una brecha de infraestructura de 170 mil millones de dólares que sigue creciendo. Si las compras del sector defensa ayudan a cerrar esa brecha, podríamos aspirar a tener un mejor PBI y un óptimo crecimiento, para luego tener unas Fuerzas Armadas correspondientes a un país de primer nivel. Es por eso que venimos trabajando esta Ley de offset, la cual se encuentra en manos de uno de los viceministerios de Economía y Finanzas y que esperamos se concluya antes de fin de año.

Por otro lado, quiero agradecer a todos los presentes, a las Armadas amigas y a las organizaciones públicas educativas y privadas, por haber participado en el V Simposio Internacional de Seguridad y Defensa, evento que está en camino de convertirse en un espacio de referencia en esta parte del mundo, ya que confluyen, en calidad de expositores, especialistas de las más diversas disciplinas, quienes convergen en el área de interés que nos ocupa: la seguridad y la defensa.

En esta oportunidad, fue nuestro deseo tocar distintos temas relacionados con la tecnología, innovación y creatividad en el campo militar y, como habrán apreciado, entre todos ellos fue posible identificar a sus comunicantes. Esto nos lleva a pensar en el enorme reto que nos espera en la gestión tecnológica de nuestras Armadas, así como en los rubros de la defensa y seguridad.

Espero que las conclusiones a las que hayan llegado enriquezcan sus conocimientos, refuercen su profesionalismo y estimule su ánimo por la investigación en este sector de la Defensa.

No obstante, un reto trazado por la Marina de Guerra del Perú es estrechar aún más los lazos de amistad, cooperación y entendimiento con las Armadas e instituciones amigas. En ese sentido, estoy seguro que la realización de este simposio ha permitido, a través de la relación entre expositores, moderadores y asistentes, la generación de fuertes lazos de amistad que perdurarán en el tiempo.

Asimismo, espero que nuestros oficiales más jóvenes capitalicen todo el conocimiento asimilado y tomen conciencia que, hoy más que nunca, la gestión de la tecnología será importante para el futuro de las organizaciones, pero en especial para las marinas, como la nuestra, cuyos roles tan variados nos obligarán a utilizar la misma plataforma y medios, en un amplio rango de actividades.

Para nuestros amigos de otros países, les deseo un feliz retorno, esperando que su estadía en nuestro país haya sido de su mayor complacencia. Lleven un especial y afectuoso saludo de mi parte a los comandantes de sus respectivas Armadas y nuestros deseos de tenerlos nuevamente en nuestro país.

Finalmente, quiero felicitar a los expositores y moderadores por su valiosa contribución al éxito de este evento y a la Escuela Superior de Guerra Naval, por el planeamiento y organización. Esperando contar con su presencia para el VI Simposio Internacional de Seguridad y Defensa SISEDE 2021, declaro clausurado el V Simposio de Seguridad y Defensa.

Muchas gracias.

V SIMPOSIO INTERNACIONAL

DE SEGURIDAD Y DEFENSA

PERÚ 2019

Tecnología, innovación y creatividad en el campo militar

ORGANIZADO POR:

Este evento contó con el apoyo de las siguientes instituciones :

colaboradores:

colaboradores academicos:

auspiciadores:

ISBN: 978-612-47941-1-7