LA CIBERDEFENSA DEL GEMELO DIGITAL EN LOS BUQUES DE LA ARMADA

Alberto GARCÍA ROMERO

(ing.)

Álvaro SANTOS GARCÍA
Ingeniero de Ciberseguridad de ISDEFE

Situación actual

HOY en día, los Estados modernos se enfrentan a diferentes desafíos que confieren a la ciberseguridad un carácter cada vez más complejo. Las nuevas tecnologías de la Industria 4.0 permiten digitalizar los procesos logísticos, optimizar los períodos de mantenimiento, predecir averías y actuar antes de que estas se produzcan. Tener que procesar, supervisar y almacenar los datos de estos procesos industriales ha creado una necesidad de convergencia entre sistemas de tecnologías de información (TI) (1) y de tecnologías de operación (TO) (2). En los últimos años, y en muchas ocasiones como consecuencia de la evolución de los escenarios bélicos tradicionales a la ciberguerra, estas infraestructuras han estado en el punto de mira de los ciberdelincuentes.

Uno de los ejemplos de ciberataques más recientes a una infraestructura de esta naturaleza se produjo dentro del contexto de la guerra entre Rusia y Ucrania. El Industroyer2 fue un ciberataque en el que un grupo de ciberdelincuentes rusos consiguió acceder e insertar un *malware* en la red de control industrial de una subestación eléctrica a través de su red TI, provocando un corte de suministro eléctrico en una región ucraniana.

(1) TI: sistemas que se centran en el uso de los datos como información.
(2) TO: sistemas que interactúan con el mundo físico (sensores, actuadores).

La convergencia de los sistemas TI y TO en los buques más modernos de la Armada supone un reto a la hora de diseñar e implementar las medidas de ciberseguridad que puedan hacer frente a las nuevas amenazas y permitan la operación de los sistemas embarcados con garantías.

Desde el punto de vista de la seguridad, para explotar las vulnerabilidades de una red de control aislada en los buques más antiguos era necesario acceder físicamente al objetivo, y no se consideraba su ciberseguridad como un aspecto relevante a tratar; pero una vez se encuentran los sistemas conectados entre sí, la facilidad de acceso a través de internet, moviéndose lateralmente de un sistema a otro, cambia las reglas del juego.

Si no se establecen las medidas de protección suficientes, un atacante a través del ciberespacio podría ser capaz de acceder y manipular el sistema de combate de un buque de guerra a miles de kilómetros de distancia. El ciberespacio se ha convertido en un nuevo campo de batalla, cuyas amenazas pueden producir un fuerte impacto en cualquier infraestructura informática. Día a día, las Fuerzas Armadas se especializan cada vez más en este nuevo dominio, entre ellas la Armada.

Con el objetivo de mejorar las capacidades de las unidades de la Fuerza frente a las amenazas en el ciberespacio, se establece la Directiva 3/2021 del AJEMA. En ella se define que las unidades de la Flota operarán en un ámbito multidominio donde tendrán que enfrentar las amenazas existentes en el ciberespacio para el desarrollo favorable de las operaciones, y para mejorar la capacidad de ciberdefensa de los sistemas, se deberá contemplar esta desde su diseño en las primeras fases del ciclo de vida de la adquisición de nuevas unidades.

En la actualidad, la Armada se encuentra en un proceso de transformación digital que permitirá operar con ventaja en entornos disputados mediante la superioridad tecnológica y de la información. La transformación digital no solo supone un salto tecnológico, sino también un cambio de mentalidad para apoyar a los buques del futuro, adaptando los procesos de trabajo logísticos al nuevo entorno normativo, industrial y tecnológico. A pesar de sus grandes ventajas, también implica incrementar la superficie vulnerable a las amenazas existentes en el ciberespacio. Uno de los sistemas que mejor representa el concepto de transformación digital y la convergencia de los mundos TI y TO es el Gemelo Digital.

El Gemelo Digital

Es una representación virtual de un buque real que recibe información relevante de sus sistemas, la cual podrá ser almacenada y explotada para dar soporte a diversos procesos de decisión en operaciones y sostenimiento del buque. El Gemelo Digital añade la información de los sensores de los equipos, lo que proporciona una visión dinámica y a tiempo real del buque.

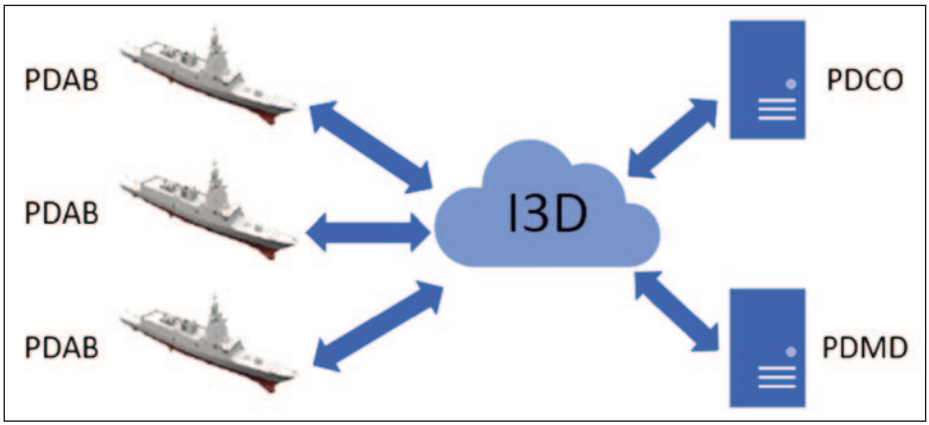
Ejemplo de interfaz del Gemelo Digital. (Fuente: Navantia)

Para las unidades de nueva construcción se pretende desarrollar un Gemelo Digital específico, con su propia configuración para cada una. A su vez, existirán tres plataformas sincronizadas durante todo el ciclo de vida donde residirá el Gemelo Digital:

— La Plataforma del Gemelo Digital del Contratista (PDCO), que proporcionará apoyo al diseño, construcción, pruebas, sostenimiento y mejora continua del producto durante todo su ciclo de vida.
— La Plataforma del Gemelo Digital del Ministerio de Defensa (PDMD) se encargará de almacenar, analizar y consolidar los datos de interés, estáticos y dinámicos de la clase, y tendrá labores de soporte.
— La Plataforma del Gemelo Digital A Bordo (PDAB) albergará información del buque donde se encuentre embarcada y dará soporte a las aplicaciones operativas, logísticas y de alistamiento a bordo, interactuando con sus sistemas.

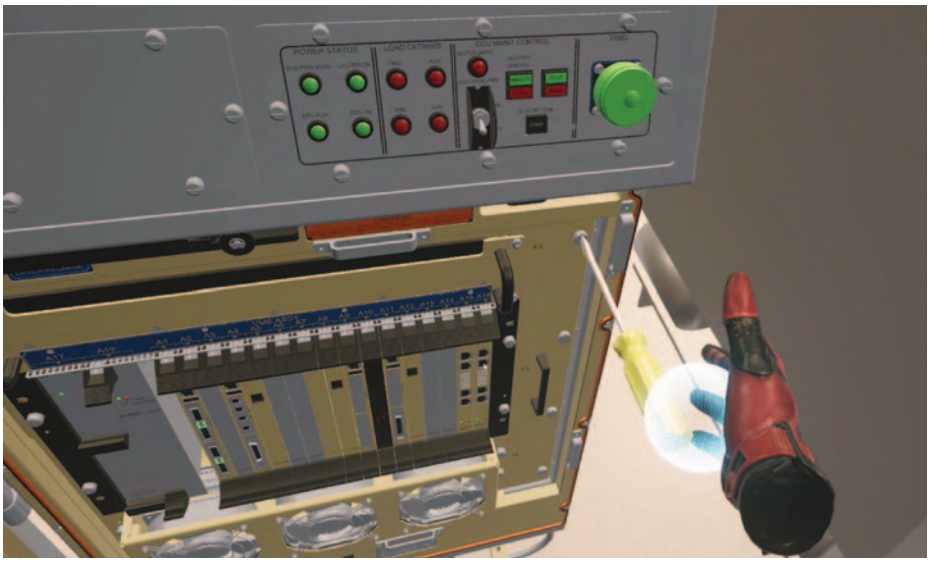
El Gemelo Digital proporcionará diversos servicios de usuario, dividiéndose estos en tres tipos fundamentales:

— Servicios de apoyo logístico, con el objetivo de facilitar y guiar a la dotación en la gestión y realización de estas tareas con el uso, por ejemplo, de realidad aumentada o realidad virtual.



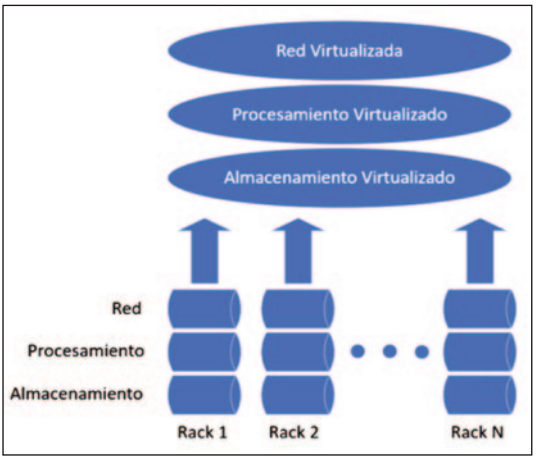
Plataformas del Gemelo Digital. (Elaboración propia)

— Servicios de apoyo a la operación, como pueden ser de eficiencia energética, esfuerzo de dotaciones o el de asistencia a la navegación y derrota.
— Servicios de adiestramiento, que proporcionarán capacidades de adiestramiento, a bordo y en tierra, en relación al control de plataforma, sistema de combate y navegación.



Ejemplo de la función de adiestramiento del Gemelo Digital. (Fuente: Navantia)

El Gemelo Digital es un sistema innovador no solo por la gran variedad de funciones que posee, sino que también utilizará paradigmas tecnológicos vanguardistas que permitirán explotar el sistema de manera eficaz.



Hiperconvergencia. (Elaboración propia)

Su diseño estará definido con el modelo de arquitectura basada en una infraestructura hiperconvergente, definida y unificada mediante *software*, en la que cada elemento *hardware* de proceso o almacenamiento tradicional (por ejemplo, un disco duro) aportará sus recursos de forma combinada al conjunto del sistema, funcionando como un único nodo virtualizado. Todas las funciones del sistema se ejecutarán en esta capa de *software* (representación virtual del almacenamiento y procesamiento físico) en lugar de seleccionar componentes *hardware* específicos para cada función.

Una infraestructura hiperconvergente proporciona beneficios en relación al coste (se utiliza menos *hardware* y el que se usa es comercial), la gestión centralizada (funciona como un único nodo y se gestiona a través de una interfaz) o la escalabilidad del sistema (se pueden añadir recursos sin perjudicar su operación), pero también supone un desafío en cuanto a ciberseguridad. A pesar de que el Gemelo Digital, gracias a su infraestructura hiperconvergente, poseerá intrínsecamente mecanismos de seguridad y tolerancia a fallos, se deberá aplicar una estrategia de seguridad orientada a las amenazas de los sistemas *cloud* (en la nube). El Gemelo Digital combinará una solución de nube *on-premise* (físicamente localizada en el buque en la PDAB) con matices de nube híbrida, ya que también estará desplegado y sincronizado en la PDCO y en la PDMD. Algunas de las principales amenazas a las que se enfrenta este tipo de sistemas pueden ser la débil protección de la información, las llamadas entre aplicaciones inseguras o una mala identificación y autenticación remota de los usuarios en el sistema.

Evolucionar de los sistemas TI clásicos —a los que ya estamos acostumbrados— a estas nuevas arquitecturas no es un proceso sencillo. Se deberán adaptar las medidas de ciberseguridad tradicionales a estos nuevos esquemas, pero sin dejar de lado todo lo aprendido previamente. Se utilizará como referencia la norma *CCN-STIC-220 de Arquitecturas Virtuales*, desarrollada en julio de 2020 por el Centro Criptológico Nacional (CCN), que recoge las medidas de seguridad que se deben aplicar a los sistemas de esta naturaleza.

Ciberdefensa del Gemelo Digital

Como todo sistema complejo, se debe concebir aplicando la idea de la seguridad desde el diseño. Se introducirán controles de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información, así como sus interconexiones con otros sistemas, donde residen las mayores vulnerabilidades en los buques de guerra (3).

Protección de las comunicaciones

En términos generales, una interconexión se produce cuando se habilitan flujos de comunicaciones físicos o lógicos que permiten intercambiar información entre dos o más sistemas de diferente nivel de seguridad.

Para su correcto funcionamiento, el Gemelo Digital obtendrá información de los sensores pertenecientes a otros sistemas distribuidos en el buque para proporcionar al operador una visión a tiempo real. En consecuencia, se deberá proteger la información que viaja a través de esas interconexiones cumpliendo una serie de principios básicos de ciberseguridad. Con esta problemática en mente, el Gemelo Digital deberá tratar al resto de sistemas con los que estará interconectado como entornos no confiables, siendo necesaria la implementación de medidas de seguridad para el intercambio de información (principio clásico del nodo autoprotegido). Estas medidas tendrán que cumplir con la normativa de seguridad vigente, en este caso la CCN-STIC, con el objetivo de impedir la propagación de incidentes de ciberseguridad entre sistemas y mitigar su impacto en la misión del buque.

Para proteger los flujos de información entre el Gemelo Digital y otros sistemas, se desplegarán dispositivos de protección perimetral (DPP) que actuarán como mediadores entre los puntos de entrada y de salida de la interconexión entre sistemas. Dependiendo del diseño o del grado de clasificación de la interconexión, puede ser necesario el uso de dos o más DPP, que generarán un sistema de protección perimetral.

Con el fin de reducir la superficie de exposición a las amenazas, se deberán desplegar los elementos imprescindibles para satisfacer los requisitos de funcionamiento de la interconexión. Cada DPP cumplirá un rol en la protección del flujo de información, de manera que existan varias líneas de defensa frente a un posible ataque (principio clásico de defensa en profundidad). Por ejemplo, un cortafuegos puede trabajar varias capas del modelo TCP/IP (4) (principal-

---

(3) Combined Joint Operations from the Sea Centre of Excellence (2020, mayo): *Naval Operations-Cybersecurity Afloat*.

(4) TCP/IP: modelo de protocolos utilizado para comunicaciones en redes.

mente red y transporte), permitiendo o denegando el tráfico de paquetes IP mediante la definición de reglas (teniendo en cuenta direcciones IP de origen, destino, puertos, etc.), mientras que un *proxy* trabajará detectando e impidiendo usos anómalos de protocolos a nivel de aplicación (navegación web, correo electrónico, etcétera).

Protección de la información

Además de las comunicaciones, será imprescindible proteger la información que maneje el sistema. Una de las funcionalidades del Gemelo Digital es ayudar a la toma de decisiones mediante la visualización del estado del buque, por lo que la información tratada tendrá un nivel elevado de sensibilidad. Se deberá hacer hincapié en la confidencialidad y la integridad de la información con el fin de evitar la materialización de amenazas como su filtrado o manipulación, provocando un uso incorrecto del sistema o la toma de decisiones basadas en información que ha sido comprometida. Para proteger la confidencialidad, se utilizarán mecanismos de cifrado para el acceso, intercambio y almacenamiento de información con el objetivo de evitar cualquier acceso no autorizado a la red y la inspección de la información (almacenada o en tránsito) por parte de terceros.

Por otra parte, el sistema dispondrá de herramientas contra código dañino y mecanismos que impidan la modificación de ficheros en las bases de datos, además de dispositivos de control de acceso al sistema que ayudarán a proteger la integridad de la información almacenada. A su vez, el sistema permitirá la creación de *backups* de la información almacenada y también de las máquinas virtuales que forman el sistema.

Protección de la infraestructura (Zero Trust)

Siguiendo la estrategia de seguridad de «no confianza», se presenta un paradigma en auge en las últimas décadas: el modelo *Zero Trust* (confianza nula). Este pone el foco de la ciberseguridad en los activos en lugar de centrarse en la seguridad perimetral de la red. *Zero Trust* mantiene una estricta verificación de todos los dispositivos, usuarios y solicitudes del sistema, hayan ocurrido dentro o fuera de él. En otras palabras, no se confiará implícitamente en ningún acceso al sistema o a sus activos por parte de dispositivos, usuarios o aplicaciones, siendo necesario aplicar procesos de autenticación y autorización robustos. Esta estrategia resulta útil tanto para proteger la información del Gemelo Digital como para proteger su infraestructura y las aplicaciones del sistema.

El Gemelo Digital estará integrado con la infraestructura de clave pública del buque (PKI) y soportará una autenticación de factor múltiple. Se utilizarán

protocolos de doble autenticación, es decir, las partes que participan en la comunicación deberán demostrar que son quien dicen ser utilizando certificados digitales o sus claves de la PKI, impidiendo ataques de fuerza bruta, suplantaciones de identidad o ataques de *Man-in-the-Middle* (MitM) (5).

Se deberá verificar que todas las peticiones de acceso a las máquinas virtuales o el consumo de datos por parte de las aplicaciones son legítimas y que, además, las aplicaciones y los usuarios tienen los permisos mínimos requeridos para su funcionamiento (principio de mínimo privilegio), manteniendo de esta forma la confidencialidad de la información y la integridad de los datos. Una vez el usuario se ha autenticado en el sistema, el acceso a los datos será permitido únicamente a aquellos que tengan la «necesidad de conocer». Se utilizará una política de control de acceso basada en roles, donde se segregará a los usuarios por su función en el sistema y se proporcionarán privilegios de acceso dependiendo del rol que se desempeñe (operador, administrador, etc.), por lo que no todos tendrán los mismos privilegios sobre los datos.

Además de la fuerte identificación de los elementos del sistema, el control de accesos y la restricción de permisos, el paradigma *Zero Trust* también presenta la supervisión constante del sistema como uno de sus principios de seguridad.

Integración con el Sistema de Ciberdefensa

Al igual que el resto de sistemas del buque —como el Sistema Integrado de Control de Plataformas, el Sistema de Servicios Integrados o el Sistema de Combate—, el Gemelo Digital contará con sondas desplegadas que recolectarán eventos de seguridad generados por todos los elementos que lo forman. Un evento de seguridad es una ocurrencia en un sistema, no necesariamente maliciosa, que puede indicar actividad sospechosa de serlo. Un ejemplo de ello puede ser el *log-in* incorrecto de un usuario, una petición no permitida por el cortafuegos o el acceso denegado para leer un fichero.

Aparte de recolectar eventos, las sondas también se encargarán de enviarlos al Sistema de Ciberdefensa del buque, el cual los agregará y correlacionará mediante reglas para detectar si el evento (o conjunto de eventos correlacionados) supone un incidente de seguridad. Una vez recibida la información, los operadores del Sistema de Ciberdefensa podrán analizar y supervisar la actividad del mismo con el objetivo de detectar indicadores de compromiso (IoC) que denoten una posible vulneración de la seguridad. Conocer la situación en tiempo real de los elementos monitorizados en el buque ayuda a la dotación en la toma de

(5) *Man-in-the-Middle*: forma de ataque de escucha activa en la que el atacante intercepta las comunicaciones de datos para leer, modificar la información o hacerse pasar por una o más de las entidades involucradas.

decisiones y permite una rápida respuesta ante posibles incidentes que puedan comprometer la seguridad del buque y de su dotación.

Además del envío de información, las sondas desplegadas contarán con sistemas de detección de intrusiones (IDS) que localizarán accesos no autorizados al sistema. Ante una actividad sospechosa, los IDS emitirán una alerta al Sistema de Ciberdefensa para que se tomen medidas en respuesta al incidente de seguridad.

Conclusiones

La transformación digital supone un avance en la mejora de capacidades de las unidades de la Armada, pero también un vector de entrada de amenazas y riesgos cada vez más complejos en términos de ciberseguridad. La Armada tendrá que adaptarse a numerosos retos en el campo de las tecnologías de información y de la operación, donde la convergencia de estos sistemas en los buques crea una superficie de ataque que puede ser aprovechada por atacantes a través del ciberespacio.

Como parte del proceso de transformación digital, el Gemelo Digital materializa las amenazas inherentes de los sistemas TI que convergen con sistemas TO, convirtiéndose así en un posible objetivo por parte de actores maliciosos. Para reducir los riesgos de sufrir un ataque y su impacto en la misión, se implementarán medidas de ciberdefensa que permitan mantener la confidencialidad, integridad y disponibilidad de los datos, así como proteger las interconexiones del Gemelo Digital con otros sistemas.

En los procesos de diseño de los buques de nueva construcción, el personal de Armada, junto con la industria nacional, está trabajando para que la integración de la transformación digital en los nuevos buques se realice de manera satisfactoria y permita aprovechar la superioridad tecnológica frente al adversario para el cumplimiento de la misión. Con apoyo de la normativa de referencia nacional e internacional, se implementará la seguridad desde el diseño de los sistemas con el objetivo de explotar las nuevas tecnologías disruptivas hasta el final de su ciclo de vida, para poder operar los sistemas con garantías frente a la evolución de las amenazas del ciberespacio.

BIBLIOGRAFÍA

Díaz del Río Durán, J. (2020, junio): «Futuro Gemelo Digital (DG) de la *F-110*». Revista General de Marina, pp. 893-908.

Gálvez Reina, M. (2015, abril): «La Ciberdefensa, un reto para las FF. AA.». Revista General de Marina, pp. 473-483.

Estado Mayor de la Armada (2022, mayo): *Concepto del almirante jefe de Estado Mayor de la Armada sobre la Ciberdefensa en la Armada*.

—(2021, enero): *Directiva 3/2021 del AJEMA*.