BAM DE INTERVENCIÓN SUBACUÁTICA. PRIMER BUQUE CIBERINTELIGENTE DE LA ARMADA

Vanesa MARTÍNEZ TAMARGO

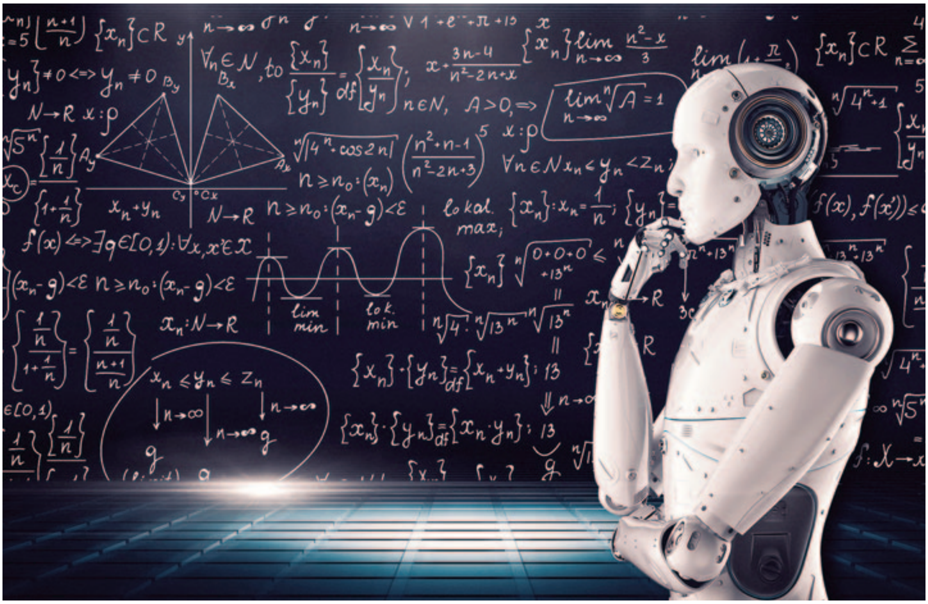
(ing.)

QUÉ es eso del doble factor de autenticación de Amazon? ¡Pero si también lo tiene Netflix! ¿Y esta nueva moda de contraseñas con mayúsculas, minúsculas y números? ¿Y por qué no los números de lotería que van a salir en Navidad? Total, si antes ya era complicado recordar cuál era mi contraseña, ahora es, si cabe, más difícil. Pues sí, eres humano… Bienvenido a una nueva era ciberdigital.

Un poco de historia

En los últimos tiempos nos inundan día sí y día también con noticias relativas a ataques cíber, entre los que destacan el secuestro de información, robo de credenciales, inhabilitación de sistemas informáticos, ciberespionaje, etc. Las empresas, de forma consciente o no, acumulan ingentes cantidades de datos que hoy en día son el nuevo «oro». Estos, altamente sensibles, se ubican en sistemas de información hiperconectados, convirtiéndolos en hipervulnerables. Cualquiera se podría preguntar qué es lo que se consigue con ello; pues bien, desde algún tipo de ganancia económica hasta conseguir información privilegiada para traficar con ella o causar daño a la imagen institucional.

El 9 de marzo de 2021 el Servicio Público de Empleo Estatal (SEPE) sufrió un ataque. Las primeras informaciones se dieron a conocer a media mañana de aquel día, y por la tarde ya se pudo confirmar que se trataba de un incidente



Inteligencia artificial. (Fuente: *www.wikipedia.org*)

relacionado con un *ransomware* (1) llamado Ryuk. El personal estuvo movilizado 24/7 durante tres semanas, pero los protocolos de ciberseguridad del SEPE no lograron frenar a tiempo el desastre. El atacante desplegó y ejecutó Ryuk en el mayor número de equipos posible, a la vez que comenzó a cifrar los archivos del organismo. La gravedad del caso fue notable.

¿Esto pasaría en el entorno naval?

Por desgracia, sí; atrás queda ya el tiempo en que se pensaba que un buque era una isla protegida de influencias externas que pudieran condicionar la operación y el correcto funcionamiento de los sistemas IT (2)/OT (3) instalados a bordo.

---

(1) *Ransomware* es un tipo de *malware* o código malicioso que toma por completo el control del equipo infectado, bloqueando o cifrando la información del usuario para, a continuación, pedir un rescate (generalmente en criptomoneda) a cambio de liberar o descifrar los ficheros del dispositivo.

(2) Tecnología de la Información: se aplica a los equipos de telecomunicación. Su ámbito suele ser el de empresas y negocios.

(3) Tecnología de la Operación: proceso físico que monitoriza y controla dispositivos.

(Fuente: www.*prosertek.com*)

NotPetya, el peor ciberataque a una flota

En 2017, Maersk sufrió pérdidas cifradas en 300 millones de dólares en el mayor ataque al sector marítimo conocido. Se trató del NotPetya, un *ransomware* global que infectó el sistema de reservas de la compañía, causando congestión en 80 puertos de todo el mundo, muchos de ellos en los que Maersk suele operar, que sufrieron una disrupción total. La terminal automatizada de Róterdam fue desactivada, y en Nueva York y Nueva Jersey varios sistemas electrónicos colapsaron. NotPetya fue un caso que hizo saltar las alarmas a nivel mundial, pero para nada aislado. Desde entonces, diversos ataques cibernéticos han trastocado la actividad de puertos y buques, dejando importantes pérdidas para las empresas.

Casi en sintonía con el *modus operandi* de 2017, en 2019 un ataque de *ransomware* afectó al puerto de San Diego, encriptando varios archivos y solicitando un rescate en *bitcoins*. Poco después, COSCO Shipping fue atacado con otro virus del mismo tipo que interrumpió la comunicación entre clientes, buques, terminales y proveedores, creando un caos en toda la costa oeste de Estados Unidos. Inmediatamente cerraron sus redes en otras regiones como medida de precaución.

A diferencia de Maersk, que tenía una red global integrada, COSCO Shipping posee un sistema segregado en varias redes ubicadas en diferentes regiones.

(Fuente: *Marine and Naval Engineering*)

Esta descentralización parece que ayudó a prevenir el efecto de propagación del ciberataque.

Haciéndose eco del refrán «cuando las barbas de tu vecino veas cortar, pon las tuyas a remojar», ENISA (Agencia Europea para la Ciberseguridad) promulgó la *Guidelines for cybersecurity in the maritime sector,* con unas directrices claras sobre la gestión de los riesgos cíber, además de una autoevaluación para marcar la madurez de los sistemas de las tecnologías de la información y la comunicación (TIC) implantados y poder obrar en consecuencia.

Ahora cabría hacernos esta pregunta: ¿por qué si saben que son un blanco fácil no protegen sus activos?

La implantación de medidas de ciberdefensa sigue siendo un proceso poco extendido; la carencia, en general, de conciencia cíber hace que los procedimientos se vean más como una traba que como un elemento del que sacar provecho. El hecho de que haya que modificar las arquitecturas tradicionales de los sistemas TIC, incluyendo los incrementos de costes en los ajustados presupuestos, hace que de manera habitual haya reticencia para su implantación. Es como creer en lo intangible, lo inefable, y si no lo veo y lo toco carece de importancia, ya que, muy a nuestro pesar, hasta que no ocurre una desgracia no se hace patente su necesidad.

Si profundizamos un poco, el ser humano sigue siendo el eslabón más débil, y no solo porque somos fácilmente «engañables», sino porque en general:

— Carecemos de formación o de recursos humanos para hacer frente a posibles ataques.
— Hay falta de protocolos para testar la capacidad real de prevención, contención e incluso mitigación.
— No gestionamos los riesgos inherentes a la ciberdefensa con los que se podrían establecer medidas técnicas específicas para prevenirlos.
— No disponemos de sistemas robustos para detener o mitigar ataques sofisticados.

¿Qué es lo que hace la inteligencia artificial?

La evolución de las técnicas de inteligencia artificial (IA), como puede ser el aprendizaje automático (*machine learning*) (4), contribuye a anticipar, neutralizar y gestionar incidentes de ciberseguridad con una mayor capacidad de reacción y efectividad mediante el análisis de gran cantidad de información sobre el contexto y sin la necesidad de intervención humana altamente especializada. Por otro lado, nos ayudan a través de «sistemas de ayuda a la decisión», mediante los que se nos ofrecen diferentes alternativas a cualquier problema que pueda surgir; como resumen, se destacan los siguientes:

— *Big data/data lakes*: con la gestión masiva de información se prioriza qué situaciones y ataques tienen prioridad de gestión y cuáles son falsos positivos, ya que hay veces que la máquina no es capaz de discernir entre un ataque real y los que no lo son; por ello, a través del aprendizaje automático nuestro sistema es capaz de detectar las diferencias, actuando en consecuencia y, con ello, minimizando la carga de trabajo de los sistemas, con lo que la respuesta puede ser más eficaz y rápida.
— *Generación de respuestas en tiempo real*: permite tomar acción inmediata en los ataques para minimizar riesgos, basándose en infinidad de datos previos y de contexto, los cuales se han clasificado y etiquetado como nocivos para el sistema.
— *Automatización*: usando técnicas de *machine learning*, nuestros sistemas pueden no solo aprender de ellas, sino que también logran identificar ataques *zero-day* (5) basándose en patrones de comportamiento anteriores, lo cual permite una respuesta automática a muchas de las

(4) El *machine learning* es una disciplina del campo de la inteligencia artificial que, a través de diferentes algoritmos, es capaz de aprender. De esta manera, con el análisis de datos es capaz de identificar patrones en datos masivos y elaborar predicciones (análisis predictivo) y, en consecuencia, prevenir futuros ataques.

(5) El *zero-day* es un *exploit* que se aprovecha de una vulnerabilidad de seguridad todavía desconocida por la comunidad de ciberseguridad. En muchos casos, el código de explotación lo

amenazas, identificando incluso otras novedosas, potenciando así la detección y respuesta.
— *Predicción y prevención*: basándonos en los apartados anteriores, nos ayuda a mejorar el análisis forense de los ataques ejecutados, lo que se traduce en una mejora continua y, con ello, la de nuestras defensas.

¿Entonces, la inteligencia artificial es la solución a mis problemas?

Se podría decir que la inteligencia artificial es la panacea… pero lamentablemente no lo es. Es innegable que es un método eficaz para reducir el impacto de los ciberataques. El conocimiento de los expertos humanos se integra para la toma de decisiones y la prevención, manejando un mayor abanico de opciones, a veces impensables. Sin embargo, la inteligencia artificial aplicada a ciberataques puede facilitar el proceso de escalada para causar ataques más rápidos, inesperados, sofisticados e impactantes. Se aprende de las vulnerabilidades y de las soluciones a ataques anteriores, mejorándolos, haciéndolos más precisos e inteligentes y encontrando puertas traseras donde antes no las había.

La pregunta del millón es ¿... y cómo lo hacemos?

La infraestructura de red no ofrece directamente seguridad, pues es necesario disponer de una arquitectura de red convergente con las redes de datos. Esto se consigue utilizando un conjunto de barreras que permita que cuando falle una solución se mantengan otras que la protejan.

Hay varios elementos pasivos o activos que son capaces de aprender del entorno y actuar en tiempo real y, a su vez, identificar posibles amenazas, ayudando al operativo a la toma de decisiones. A continuación, se enumeran los más conocidos:

— *Firewall (FW)*: es el elemento más básico; se encarga de analizar, paquete a paquete, todo el tráfico que entra o sale de nuestra red; es decir, es la primera medida de seguridad que se aplica cuando queremos proteger una red.
— *NGFW (Next Generation Firewall)*: se denomina así a los FW de nueva generación y son el siguiente escalón a los tradicionales FW. Dependiendo

escribe la misma persona u organización que descubrió la vulnerabilidad. Se trata de una de las amenazas más serias, ya que abre una ventana de vulnerabilidad de los sistemas desde el momento en que se desarrolla el *exploit* hasta que la vulnerabilidad es parcheada.

del modelo, pueden actuar en la capa 7 (6), 5G, tienen capacidad de IPS/IDS (sistemas de detección de intrusos), incluyen algoritmos y son capaces de detectar amenazas *zero-day*, filtros de navegación *web*, concentrador VPN IPSec (7) , además de bloqueo de amenazas avanzadas o gestión de vulnerabilidades.

— *WAF (Firewall de Aplicación Web)*: es un dispositivo de seguridad diseñado para analizar el tráfico de datos en las aplicaciones *web*, monitorizándolas para detectar posibles fisuras de seguridad.
— *IPS/IDS*: es una aplicación de *software* destinada a la detección, en dispositivos o en una red, de accesos no autorizados.
— *NIDS/NIPS (Sistema de Detección de Intrusos de Red)*: monitoriza la actividad de la red; podría, por ejemplo, cortar la conectividad de todo un segmento de red si este se encuentra comprometido.
— *HIDS/HIPS (Sistema de Detección de Intrusos de Host)*: monitorizan la actividad de un *host*. Podría, en su caso, cerrar puertos de un servidor si este se encuentra comprometido a través de una conexión por dicho puerto.
— *DAM/DAF (Monitorización de Bases de Datos)*: son capaces de descubrir y gestionar vulnerabilidades, monitorear la actividad de auditoría, la prevención de intrusiones basada en políticas de seguridad (lista blanca o negra) y la gestión de acceso de usuarios y administradores. Se garantiza la integridad de los datos sin afectar al rendimiento.
— *SIEM (Sistema de Gestión de Eventos e Información de Seguridad)*: permite recopilar, normalizar y correlacionar eventos de seguridad, proporciona inteligencia de seguridad, descarta falsos positivos, evalúa el impacto de un ataque, unifica la gestión de la seguridad, centraliza la información e integra herramientas de detección de amenazas.

¿Cuáles son las diez principales amenazas emergentes de ciberseguridad según la Agencia de la Unión Europea para la Ciberseguridad (ENISA)?

— Compromiso de la cadena de suministro de dependencias de *software*.
— Campañas de desinformación avanzada.
— Aumento del autoritarismo de vigilancia digital/pérdida de privacidad.

---

(6) Es la capa superior del procesamiento de datos con las que interactúan los usuarios. Por ejemplo, las solicitudes y respuestas utilizadas para cargar páginas *web* son eventos de la capa 7. Los ataques de denegación de servicio (DDoS) suelen tener lugar en este nivel.

(7) Se trata de redes virtuales privadas las cuales utilizan un conjunto de reglas o protocolos de comunicación para configurar conexiones seguras a través de una red. El protocolo de internet (IP) es el estándar común que determina cómo viajan los datos por internet. IPSec agrega cifrado y autenticación para hacer que el protocolo sea más seguro.

— Error humano y sistemas heredados explotados dentro de ecosistemas ciberfísicos.
— Ataques dirigidos mejorados por datos de dispositivos inteligentes.
— Falta de análisis y control de infraestructura y de los objetos basados en el espacio.
— Aumento de amenazas híbridas avanzadas.
— Escasez de habilidades cibernéticas.
— Los proveedores de servicios de TIC transfronterizos como único punto de fallo.
— Abuso de inteligencia artificial con fines maliciosos.

BAM IS. Nuestro primer ciberbuque inteligente

El BAM IS será el primer buque de la Armada que aúne estas capacidades en el momento de su entrega a la Armada en 2025. La ciberdefensa ha sido tenida en cuenta desde las primeras fases de proyecto; en septiembre se superó la fase de Revisión del Diseño Preliminar Inicial (IPDR), que permite comenzar con el diseño funcional del buque, sin que los sistemas estén definidos a un nivel granular de ingeniería. A continuación tendrá lugar la Revisión Preliminar del Diseño (PDR); con ella se avanza a la concreción del proyecto a un mayor nivel de detalle.

(Fuente: Oficina de Programa BAM IS)

En mi barco, ¿qué es susceptible de ser atacado?

- *Sistema de Combate (SCOMBA)*: puede tener acceso a redes que tratan información clasificada, aprovechando alguna vulnerabilidad. Este buque no es objeto de sistemas de armas como el Aegis de las fragatas, pero no hay que olvidar que los sensores tienen la mala costumbre de calentarse. Interactuando sobre el sistema de refrigeración por agua técnica del SICP (8), por ejemplo, a través del SICP se pueden sabotear los sensores.
- *Sistema Integrado de Control de Plataforma (SICP)*: a través de un ataque DDoS (9) (denegación de servicio), pongamos por caso, se podrían sobrecargar las redes del sistema con datos, de forma que los sistemas no los puedan procesar, dejando inoperativos los servicios a equipos vitales y a sistemas contraincendios, de refrigeración, de lubricación y combustible, etcétera.
- *Sistema de Posicionamiento Dinámico (DP)*: este tiene un algoritmo propio que controla automáticamente el rumbo y la posición de un barco mediante los propulsores, basándose en los datos recibidos de los GPS, giros, inerciales, anemómetros y MRU (*Motion Reference Unit,* dispositivo que mide cabeceo, balanceo y desplazamiento vertical del buque). En 2008, la Autoridad General del Faro del Reino Unido e Irlanda realizó, a efectos de prueba, el *jamming* (10) de un área oceánica dentro de la cual se encontraba uno de sus buques boyeros, afectando al AIS *(Automatic Identification System)*, al DP con la descalibración del giróscopo, al sistema de comunicaciones digitales y no actualización en tiempo real de la cartografía electrónica (11).
- *Sistema de Intervención Subacuática*: utiliza redes wifi para comunicarse con el centro de control de operaciones, así como con el operador de los equipos de intervención subacuática (EIS). Estas redes son muy vulnerables, ya que con un ataque tipo MITM (12) (*Man in the Middle*) se

---

(8) SICP: sistema que gestiona y controla todos los sistemas auxiliares del buque, así como el control de la propulsión.

(9) DDoS: tipo de ataque que dificulta o impide el acceso de los usuarios legítimos a redes, sistemas, servicios o aplicaciones mediante la saturación y el agotamiento de los recursos.

(10) *Jamming*: técnica de interferencia intencionada que consiste en la emisión de señales de radiofrecuencia con unas características concretas y una potencia mayor que la señal objeto, con el fin de bloquear total o parcialmente la recepción de esta última.

(11) CRAWFORD CRAWFORD, James: «Ciberataque al transporte marítimo. ¿Una amenaza real o ciencia ficción?» *Revista de Marina*, n.º 970, pp. 15-23 (Chile). ISSN 0034-8511.

(12) MiTM: Forma de ataque de escucha activa en la que el atacante intercepta para leer o modificar las comunicaciones de datos para hacerse pasar por una o más de las entidades involucradas.

podrían insertar *malwares* y desviar la comunicación a sitios inseguros y por tanto jaqueables.

— *Sistema Electrónico de Ayuda a la Navegación*: la manipulación de cualquier equipo del puente —como radares, AIS, ARPA (Radar de Punteo Automático), ECDIS (Sistema de Información y Visualización de Cartas Electrónicas), GNSS (Sistema Global de Navegación por Satélite)...— puede dejar ingobernable el buque. Como ejemplo, en 2014, NCC Group intentó penetrar en la ECDIS de un importante fabricante. En el proceso se detectaron varias debilidades de seguridad, como la capacidad de lectura de código, con lo que podía ser fácilmente modificado, descargado, reemplazado o eliminado cualquier archivo almacenado en la máquina que alojaba al sistema. Con estas debilidades, el acceso a la red del Sistema Integrado de Navegación (INS) era «pan comido». Por poner otro ejemplo, en 2016 la empresa Trend Micro demostró la facilidad con la que se podían crear buques fantasma en cualquier ubicación del mundo e insertarlos en el sistema; estos serían reconocidos por los receptores como buques reales, pudiendo activar una alerta de colisión falsa, lo que obligaría a cambiar el rumbo.

— *Sistema Integrado de Comunicaciones*: al igual que el anterior, el *Global Maritime Distress and Safety System* (GMDSS) (13) o los receptores de las señales satélites comerciales, etc., es susceptible de sufrir un ataque como los descritos anteriormente, dejando al buque incomunicado.

— *Sistemas de Posicionamiento (GPS, GNSS, Galileo PRS, etc.)*: en 2018, la vulneración del GPS fue demostrada con el ataque al *White Rose of Drachs*. Un equipo de la Universidad de Texas, en Austin, pudo tomar el control remoto del buque mediante la transmisión de señales falsas de un GPS civil. La dotación del puente acusó una desviación del rumbo establecido, por lo que se iniciaron las acciones necesarias para intentar retomarlo, sin saber que lo estaban haciendo a un rumbo equivocado y definido por los jáqueres. Los GNSS civiles en uso son mucho más vulnerables al ataque que los GPS militares, debido a que estos sistemas no utilizan metodologías de encriptación ni de autenticación.

— *Sistemas operativos (Windows, Linux, Mac OS X, Android, etc.)*: con un ataque DDoS se pueden inhabilitar los procesos de los sistemas operativos,

---

(13) GMDSS: es un conjunto de procedimientos de seguridad, equipos y protocolos de comunicación diseñados para aumentar la seguridad, facilitar la navegación y el rescate de embarcaciones en peligro. Se incluyen aquí: la baliza de indicación de posición en situación de emergencia (EPIRB-RLS); el NAVTEX, que es un sistema automático de telegrafía de impresión directa que distribuye avisos de seguridad marítima, pronósticos del tiempo, noticias y otros tipos de informaciones similares a los buques (*Maritime Safety Information*, MSI), y la red de satélites operados por Inmarsat.

Infografía con el diseño definitivo del BAM IS. (Foto: Navantia)

haciéndolos incontrolables, dejando a su vez fuera de control los sistemas sobre los que corren.

- *Sistemas de seguridad*: manipulando los circuitos cerrados de televisión (CCTV) o el control de accesos, se podrían generar múltiples alarmas simultáneas, impidiendo que el sistema las pueda procesar, y colapse.
- *Redes multiservicio sin clasificar*: por ellas circulan nuestros datos personales, listas de correo electrónico... El *phishing* es una técnica de ingeniería social para obtener información confidencial de los usuarios de forma fraudulenta; se utiliza como vector de ataque para introducirse en la red, de manera que obtiene el acceso no solo a nuestros datos personales, sino que también puede estudiar nuestro comportamiento en la red, escanear puertos para ver si alguno está abierto e incluso encontrar puertas traseras que hagan vulnerable nuestro sistema.

Tras esta retahíla de posibles vulnerabilidades, cualquier ingeniero entraría en pánico absoluto. Pero estamos de enhorabuena: la Armada ya ha previsto la forma de hacerles frente al incluir requisitos técnicos que las prevengan o minimicen.

Por tradición, nuestra arquitectura de redes es la clásica por dominios: confidencial, difusión limitada y sin clasificar; sin embargo, se le han añadido elementos y técnicas con el fin de hacerla más segura y robusta. Se destacan, entre otros:

— *Uso de fibra óptica en todas las redes del buque*: la conectividad de cobre ha sido la opción estándar que estaba disponible para cualquier tipo de conexión TIC, pero no es la correcta en cuanto a ciberdefensa. Además, de acuerdo con la *Guía CCN-STIC-154. Medidas de protección TEMPEST para instalaciones (DL),* entre las consideraciones a tener en cuenta al elegir el tipo de cableado (fibra óptica frente a cobre) se destaca la fibra óptica por su inmunidad a las interferencias electromagnéticas y por alcanzar mayores distancias sin necesidad de emplear amplificadores.

— *Añadir seguridad al estándar de acceso a la capa de enlace usando estándares IEEE 802.1x del Instituto de Ingenieros Eléctricos y Electrónicos*: tiene la capacidad de permitir o denegar la conectividad de la red según el dispositivo o la identidad del usuario; su vulnerabilidad es que solo autentifica al iniciar la conexión, con lo que podría ser utilizado por un atacante para un ataque tipo *hijacking* o secuestro de sesión. También nos sirve de referencia en la securización de redes wifi, ya que la opción de creación de túneles IPSec le añade latencia al sistema. Con el uso del estándar 802.11i mejora la seguridad sobre la autenticación y la codificación, ya que especifica el uso de AES (*Advanced Encryption Standard*), mejora la gestión de claves implementando TKIP (*Temporal Key Integrity Protocol*) y permite el uso de estándares en uso, como el 802.1x.

— *Bastionado del sistema o hardening*: es el proceso de asegurar un elemento de un sistema o al sistema en su conjunto, reduciendo sus vulnerabilidades o agujeros de seguridad, para lo que serán más propensos cuantas más funciones desempeñen. Ello implica cerrar las vías para los ataques más típicos, lo que incluye medidas como el cambio de claves por defecto, desinstalación de *softwares* superfluos, baja de usuarios inactivos o con autorización caducada, inhabilitación de accesos, servicios o funcionalidades innecesarias y fortalecer las configuraciones de aquellos que estarán en uso.

— El equipamiento *hardware/software* de los sistemas que manejen información clasificada estarán catalogados en las guías *CCN-STIC, 105. Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación* y *CCN STIC 104. Taxonomía de referencia de productos de seguridad TIC*, de manera que así nos aseguramos de que cumplen con el Esquema Nacional de Seguridad (ENS) y proporcionan un nivel mínimo de confianza de los productos o servicios adquiridos.

— *Defensa en capas*: se implementará una topología de red de múltiples capas, en la que las comunicaciones más críticas se produzcan en la capa más segura y confiable.

— *Activos ciberinteligentes en las redes*: como los descritos en el apartado anterior, estos permitirán recoger pruebas y evidencias válidas de las redes a las que se conecten, de forma que permitan la investigación del origen de un incidente y sean admisibles en un proceso legal. Dispondrán a su vez de capacidad de captura y monitorización del tráfico de red y de eventos de seguridad de todas las redes y sistemas del buque, así como la monitorización del estado del *hardware* y del *software*. Se intentará en lo posible que estos sean de diferente naturaleza con el fin último de ampliar su protección ante diferentes amenazas.

— *Listado cerrado de usuarios*: las redes y sistemas del buque deberán contar con una lista completa de usuarios. Esta deberá ser cerrada, implementándose niveles de acceso según el perfil de usuario y previendo la escalada de privilegios.

— *Nodo autoprotegido e interconexiones seguras*: en un nodo autoprotegido se marcará la directriz en el diseño, consistente en que cada sistema interconectado deberá, inicialmente, tratar al otro sistema como un entorno no confiable y deberá implementar medidas que controlen el intercambio de información con el otro sistema. Además, se deberá tener en cuenta el requisito de la transitividad (14). Si el sistema de armas está compuesto al menos por un subsistema acreditado que maneje información clasificada, las interconexiones de/desde este tendrán que realizarse acorde a norma (*CCN STIC 302*) y se deberá proporcionar una separación lógica adecuada con otras subredes/subsistemas a las que debe estar conectado el sistema: NGFW, *firewalls*, pasarelas unidireccionales (diodos), etcétera.

— *Los Sistemas de Información Clasificados y los SICP dispondrán de dispositivos de protección perimetral y de sistemas de detección y prevención de intrusiones*: con la adición a nuestras redes de los activos ciberinteligentes descritos en el apartado anterior, nos protegeremos ante intrusiones internas/externas e incluso de salidas no autorizadas al exterior.

— *Sistemas de posicionamiento GNSS con SBAS* (15) *y EGNOS* (16): con SBAS y EGNOS trabajando de forma conjunta se mejora la exactitud

(14) En una interconexión de sistemas, que a su vez están interconectados con otros sistemas, se tratará como si el sistema de mayor clasificación se conectase directamente al de menor clasificación.

(15) SBAS (Sistema de Aumentación Basado en Satélites): mejora la precisión y fiabilidad de la información GNSS corrigiendo errores de medición de señales y proporcionando información sobre la exactitud, integridad, continuidad y disponibilidad de sus señales.

(16) EGNOS (Servicio Geoestacionario Complementario Europeo de Navegación): precursor de Galileo, es un sistema mundial de navegación por satélite que se desarrolla en Europa. Consiste en una red de tres satélites geoestacionarios y una red de estaciones de anclaje terrestres encargadas de monitorizar los errores en las señales de GPS y actualizar los mensajes de corrección enviados por EGNOS. Los satélites EGNOS giran con la misma velocidad angular que la Tierra, es decir, permanecen inmóviles sobre un determinado punto sobre nuestro globo.

del GPS, ya que el sistema proporciona mensajes de corrección diferencial y datos de integridad para los satélites conjuntamente con una red de estaciones de vigilancia ubicadas en tierra (estaciones de anclaje).

— *Sistema de Posicionamiento Dinámico (DP)*: se le han incorporado unas antenas *anti-jamming,* conocidas como CRPA (*Controlled Reception Pattern Antenna*), que básicamente son matrices de antenas receptoras con capacidad para modificar sus patrones de recepción y, de esta manera, poder reducir estos en la dirección en la que se recibe la interferencia, creando un espacio nulo para evitar el *jamming*. Permite, por tanto, detectar la dirección origen de la interferencia y proporcionar una ganancia adicional de recepción de las señales reales.

Mirando hacia delante

La digitalización de todo tipo de actividades ha ampliado la superficie de exposición a posibles ciberataques de organizaciones, tanto públicas como privadas, y ha dificultado la adecuada protección de la información. Nos encontramos ante un nuevo escenario en el que el riesgo creciente de sufrir un ciberataque y su impacto potencial en la Armada no pueden ser ignorados. Tanto la realidad constatada en los ataques sufridos a navieras civiles y otros organismos del sector como los avances normativos comentados anteriormente fijan un nuevo horizonte cibernético para todos los participantes del ámbito naval.

La transformación digital es y será nuestra mayor revolución de los sistemas de la información y las comunicaciones. No obstante, a la vez será nuestro talón de Aquiles en cuanto a ciberdefensa y ciberseguridad. Extrapolando este hecho a los buques de la Armada, se han de sumar los cambios evolutivos de los sistemas más importantes del buque, como los de navegación, comunicaciones o propulsión. Para ello es preciso aunar los conocimientos especializados del sector naval con los específicos de ciberseguridad, ya que al fin y al cabo un buque es un sistema complejo que depende para su operación de multitud de subsistemas, para lograr así una mayor automatización, haciéndolos más sencillos de manejar y gestionar, pero más vulnerables.

En este sentido, la Armada ha dado un gran paso con el BAM IS, que estará preparado para hacer frente a los retos en materia de ciberseguridad y ciberdefensa que nos puedan abordar, y su botadura marcará un antes y un después.

Desde siempre los humanos hemos interaccionado con el medio, modificándolo, adaptándolo, transformándolo. Sin querer, esto se ha convertido en un desafío hombre-máquina… Pero qué sería de los humanos sin un gran reto.

Finalizo con una cita de Víctor Hugo: «Lo que conduce y arrastra al mundo no son las máquinas, sino las ideas».

BIBLIOGRAFÍA

ABAIMOV, Stanislav; MARTELLINI, Maurizio: *Cyber Arms: Security in Cyberspace*. CRC Press, 2020.
TSUKERMAN, Emmanuel: *Machine Learning for Cybersecurity Cookbook*. Ed. Packt 2019.
ACKERMANN, Pascal: *Industrial Cybersecurity*. Ed. Packt, 2021.
SMITH, Paul: *Pentesting Industrial Control Systems*. Ed. Packt, 2021.
EAGAR, Gareth: *Data Engineering with AWS*. Ed. Packt, 2021.
MAÍLLO, Juan Andrés: *Hackers*. Ed. Ra-Ma, 2020.
SMUHA, Nathalie A.: *The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence*. Agosto, 2019.
TADDEO, Mariarosaria; MCCUTCHEON, Tom; FLORIDI, Luciano: *Trusting Artificial Intelligence in Cybersecurity is a Double-edged Sword,* 2019.
BILAL, Alhayani; HUSAM JASIM, Mohammed; IBRAHIM ZEGHAITON, Chaloob; JEHAN SALEH, Ahmed: *Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry*, 2021.
YAMPOLSKIY, Roman V.; SPELLCHECKER, M. S.: *Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures*.
MARTÍNEZ TAMARGO, Vanesa: *Ontología para la Representatividad de la Ciberseguridad*. Tesis de Máster en Inteligencia Artificial. ETSI Informáticos. Universidad Politécnica de Madrid.
CABALLERO VELASCO, Ángeles: *Ciberseguridad y Transformación Digital*. Ed. Anaya.
CCN CERT, *https://www.ccn-cert.cni.es/*
Empresa Nacional de Innovacion, S. A. (ENISA)*: Cyber Risk Management for Ports. Guidelines for cybersecurity in the maritime sector*. Diciembre 2020.
«El ciberataque al SEPE provocó que sus técnicos trabajaran 19.000 horas extras en jornadas maratonianas y festivos: así levantaron una barricada contra el *ransomware*». *Business Insider, https://www.businessinsider.es/vivio-ciberataque-sepe-dentro-19000-horas-extra-973861*
«Crecen los ciberataques en la industria marítima». *Prosertek*, *https://prosertek.com/es/blog/ciberataques-en-la-industria-maritima/·*
«Cosco Shipping golpeada por ataque cibernético», *http://rm-forwarding.com/2018/07/27/cosco-shipping-ataque-cibernetico/*
Oficina de Programa BAM IS.
«La Agencia de Ciberseguridad de la Unión Europea (ENISA) destaca las principales amenazas de ciberseguridad que probablemente surjan para 2030», *https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2022/Noviembre/Noticia-2022-11-14-las-principales-amenazas-de-ciberseguridad-para-2030.html*
https://marineandnavalengineering.com/articulos/riesgo-cibernetico-maritimo/
«Ciberseguridad es uno los desafíos que plantea la transformación digital marítimo-portuaria», *https://portalportuario.cl/ciberseguridad-uno-de-los-desafios-que-plantea-la-transformacion-digital-maritima/*
The Guidelines on Cyber Security Onboard Ships Version 2.0, *http://www.ics-shipping.org/docs/defaultsource/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16*, obtenido de la red.
OMI-Comité de Seguridad Marítima (CSM) (junio 2016, 2017): Resolución MSC.428(98). «Gestión de los Riesgos Cibernéticos Marítimos en los Sistemas de Gestión de la Seguridad», *https://www.imo.org*
Organización Internacional de Normalización ISO y Comisión Electrotécnica Internacional CEI: Norma ISO/IEC 27001 (febrero 2018). «Information technology-Security techniques-Information security management systems».
Futurenautics Maritime, 2018: «Encuesta de Conectividad de la Tripulación, estadísticas de ciberseguridad y capacitación».
NIST (Instituto Nacional de Estándares y Tecnología, Estados Unidos), *https://www.nist.gov/cyberframework*
Ministerio de Asuntos Económicos: Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y Transformación Digital.

GRUFLEX-22. (Foto: José Antonio Tortolero Sara)