Ciberatacando un buque de guerra: en la búsqueda de un sistema de ciberdefensa a bordo

Autor: Bayón Laguna, Jesús

Director/es: Zamorano Pinal, Carlos; Fondo Ferreiro, Carlos.

Contacto: baylagchus@hotmail.com

Resumen:

La crisis actual en Ucrania está dejando en evidencia la importancia en la capacidad de los Estados para poder llevar a cabo ciberataques que pueden ser decisivos en un determinado momento. Esto les puede permitir llevar la iniciativa en el campo de batalla y tener efectos colaterales en el resto de los dominios físicos: terrestre, marítimo y aeroespacial.

Los buques emplean cada vez más, tecnología altamente avanzada para poder desarrollar sus cometidos y misiones. Son todo tipo de sistemas, algunos de ellos conectados a Internet. Sistemas tecnológicos de última generación que le proporcionan las capacidades operativas adecuadas para desarrollar su misión en el teatro de operaciones. Sistemas, como, por ejemplo, los integrados de control de comunicaciones, de control de la plataforma o de combate. En muchos casos interconectados entre sí.

El aumento en los últimos años de los ciberataques, el avance en nuevas técnicas, tácticas y procedimientos, y la cada vez más especialización y capacidad de ataque de grupos avanzados persistentes, en muchos casos financiados por los Estados, hace reflexionar sobre la necesidad de disponer sistemas adecuados de ciberdefensa en los buques de guerra que les haga ciber resilientes ante las amenazas en el ciberespacio.

En este trabajo se realiza un estudio detallado de los diferentes sistemas a bordo de un buque de guerra susceptibles de ser ciberatacados, para posteriormente proponer un sistema de ciberdefensa, dentro de un marco teórico, que permita la detección, monitorización y protección de los sistemas a bordo.

Palabras clave: Buque de guerra, Ciberataque, Ciberespacio, Ciberdefensa, Sistema.

---

1. Introducción

Los buques emplean cada vez más, tecnología altamente avanzada con que poder desarrollar sus operaciones, cometidos y misiones. Son todos tipos de sistemas (IT/OT[1]), algunos de ellos interconectados a Internet. Podemos pensar en cualquier tipo de sistema, desde los de comunicaciones hasta los de control de la plataforma. Los buques de guerra, además de los anteriores, emplean sistemas inherentes a su idiosincrasia, como es el sistema de combate entre otros.

Se estima que existen 50.000 barcos navegando al mismo tiempo en un momento dado, siendo todos ellos altamente vulnerables a ciberataques [1]. En 2015, expertos en ciberseguridad presentaron en una demostración lo fácil que es hackear un buque [2]. Encontraron agujeros de seguridad en los Sistemas de Posicionamiento Global (GPS; en inglés, Global Positioning System), Sistema de Identificación Automática (AIS; en inglés, Automatic Identification System, Sistema de información y visualización de cartas electrónicas (ECDIS; en inglés, Electronic Chart Display and Information System), este último utilizado para visualización de cartas náuticas.

Más recientemente, según se ha informado por diferentes medios de comunicación, a través de agencias de inteligencia, Rusia ha sido capaz de hackear al proveedor estadounidense de comunicaciones satélite Viasat el día de la invasión de Ucrania [3].

De todas las amenazas comentadas anteriormente no se escapa el buque de guerra. El impacto operativo que podría tener la pérdida, aunque sea momentánea, de las comunicaciones satelitales en el teatro de operaciones sería muy alto, ya que esto implicaría también la pérdida de redes y sistemas de mando y control principales o la pérdida de comunicación con los Cuarteles Generales. Sin mencionar tampoco, que se vea afectado el posicionamiento de un buque o algún mal funcionamiento del sistema integrado del control de plataforma.

El aumento en los últimos años de ciberataques, y la especialización cada vez más y capacidad de ataque de grupos de Amenaza Avanzada Persistente (APT[2]; en inglés; Advanced Persistent Threat) en el ciberespacio, en muchos casos financiados por los Estados, hace reflexionar en tener sistemas adecuados de ciberdefensa en los buques.

Ante la necesidad de dotar con sistemas de ciberdefensa a las nuevas unidades y plataformas que formarán parte de las Fuerzas Armadas, el Ministerio de Defensa crea a principios del año 2021 el departamento de Jefatura de Sistemas Satelitales y de Ciberdefensa dependiente la Dirección General de Armamento y Material (DGAM). Este nuevo departamento permitirá aportar una visión unificada para la obtención de sistemas de ciberdefensa.

Hasta el momento los buques de guerra de la Armada, al igual que otras Armadas y Marinas, no habían contemplado la implantación de sistemas de ciberdefensa a bordo. El punto inflexión sobre este punto de vista surge con el proyecto de las F-110, donde ya se contempla desde la fase conceptual del

[1] La Tecnología de la Información (IT) se caracteriza por la aplicación de equipos de telecomunicación como ordenadores para tratar datos. IT Suele utilizarse en el ámbito de los negocios y las empresas. En cambio, la Tecnología de las Operaciones (OT) está dedicada a detectar o cambiar los procesos físicos a través de la monitorización y el control de dispositivos también físicos, como tuberías o válvulas.

[2] Una Amenaza Avanzada Persistente es un tipo de ataque sofisticado, que se ejecuta durante un largo periodo de tiempo y está dirigido específicamente a una Organización. Normalmente se trata de un ataque selectivo de ciberespionaje o cibersabotaje llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política.

programa de un sistema de ciberdefensa a bordo. Además, éste se haría extensivo a los submarinos tipo S-80 [4].

En el ámbito internacional, ya por 2015 la Marina de EE.UU se planteó la instalación de sistemas de ciberdefensa enfocados principalmente para la protección de sus sistemas de propulsión y de energía eléctrica [5]. También existen otras Marinas preocupadas en este nuevo dominio. Ejemplo de ello es la Marina alemana, que con apoyo de la empresa Thales, va a implementar sistemas de ciberdefensa en la construcción de las fragatas tipo F-126 (MKS 180) [6]. También la Marina Nacional francesa (en francés; Marine Nationale) contempla en sus proyectos de las fragatas FDI (en francés; Fregate de defense et d´intervention) la ciberseguridad por diseño, integrando lo que han llamado un Sistema de Gestión de Ciberseguridad (CyMS; en inglés; Cyberscurity Managment System) lo que permite al buque ser ciber-resiliente [7].

1.1. Objetivos

Este trabajo plantea la consecución de una serie de objetivos estrechamente relacionados con lo expuesto en anteriormente. Dado que el buque de guerra moderno depende de redes y sistemas con tecnología de última generación (IT/OT) para poder llevar a cabo el cumplimiento de su misión, los cuales se ven expuestos a todo tipo de amenazas en el ciberespacio, el objetivo general que se plantea es definir una posible solución de diseño para la implantación de un sistema de ciberdefensa a bordo que permita la detección, monitorización y protección de los sistemas a bordo de los buques de la Armada.

A raíz de este objetivo general se fijan los siguientes objetivos específicos:

- Identificar las diferentes amenazas que existen en el ciberespacio y que pueden tener impacto en los buques de guerra.
- Describir los sistemas y redes implantados en el buque modelo (fragata F-110).
- Identificar las vulnerabilidades que presentan las redes y sistemas del buque de guerra en general, aplicados en el buque modelo.
- Estudiar la tecnología y los requisitos que debe cumplir el sistema de ciberdefensa.

2. Desarrollo

La primera parte del trabajo se centra en dar a conocer una visión general de las amenazas existentes en el ciberespacio, realizando inicialmente un estudio de los ciberinicidentes y ciberataques conocidos en las últimas décadas en el sector marítimo. La siguiente muestra un resumen de ellos, así como sus consecuencias.

Año	Ciberincidente/Ciberataque	Consecuencias
2010	Ciberataque a una plataforma petrolífera de Corea del Sur	19 días de inutilización y pérdidas de 700.000 dólares/día
2011	Ciberataque a la naviera iraní IRISL	Pérdida de contenedores
2012	Ciberataque a la plataforma petrolífera “Noble Regina” en construcción	Afectó a 89 trabajadores, estructura de apoyo y pérdidas económicas al astillero.
2013	Supuesto ciberataque del sistema ECDIS de un dragaminas de la US Navy	Encalla en arrecifes de coral cuando navegaba en el mar de Sulú, al sur de la isla filipina de Pawalan

2013	GPS Spoofing (Universidad de Austin, Texas)	El yate "White Rose of Drax" recibe durante 30 minutos señales falsas de GPS mientras navegaba en el Mediterráneo.
2017	Sistema de navegación a buque mercante	Carguero pierde acceso al sistema de navgeación durante 10 horas cuando navegaba rumbo Yibuti. Piratas somalís abordan el buque.
2017	Ciberataques a los sistemas de navegación de dos buques de guerra de la US Navy desplegados en el pacífico	Ambos sufren colisiones con otros buques mercantes. Se pierden 17 vidas humanas.
2017	GPS Spoofing	20 buques informan de anomalías en su posición de GPS cuando navegaban en el mar Negro. Todos fueron situados en una misma posición, el aeropuerto de Gelendzhik (Rusia), muy próximo a la zona de navegación.
2019	Buque con destino Nueva York alerta de incidente con impacto significativo en sus redes y sistemas.	El análisis realizado por la Guardia Costera (U.S. Coast Guard), concluye que el malware degradó significativamente la funcionalidad de los sistemas a bordo.
2020	Ransomware Hermes 2.1	Múltiples estaciones de trabajo en las redes de administración del buque se vieron afectadas

Tabla 1. Resumen de ciberinicidentes/ciberataques conocidos en el sector marítimo

Seguidamente se identifican las diferentes amenazas que existen en el ciberespacio y que pueden tener impacto en los buques de guerra. El interés de los diferentes actores o agentes amenaza en el ciberespacio no tiene límites ni fronteras. Es cierto también, que no todos disponen de los mismos recursos para poder llevar a cabo un ciberataque. Son los Estados los que se han dado cuenta del potencial que pueden tener las acciones ofensivas en el ciberespacio y los efectos que puede causar en el adversario. Muchos a través de sus propios medios o de proxies[3] efectúan acciones en lo denominado "zona gris[4]". Esto les permite fijar objetivos, prepararse con tiempo necesario y en el momento adecuado llevar a cabo sus acciones ofensivas. Tampoco nos podemos olvidar del "insider" o actor interno, especialmente de aquel que está descontento con la organización, y quién podría tener acceso directo a los diferentes sistemas del buque. Ambos, aunque también otros cierbactores pueden causar estragos a un buque en zona de operaciones si el ciberataque tuviese existo.

Lo comentado hasta el momento supone un cambio de paradigma para las operaciones militares. El ciberespacio es un nuevo dominio, que es transversal a los dominios físicos y donde además pueden tomar parte un gran abanico de ciberactores. Tal como demuestra la tabla 1 el sector marítimo no está exento de todo ello. Pensar que los buques de guerra son inmunes a ellos dado que emplean cifradores y canales específicos de comunicaciones puede ser hasta un poco temerario e ingenuo al mismo tiempo. Es por ello, que existen dos tipos de buques: "los que ya han sido ciberatacados y los que lo serán".

[3] Organizaciones privadas o instituciones que son financiadas por Estados en apoyo a ese gobierno para lograr su objetivo geopolítico, económico o militar.

[4] Zona del espectro de los conflictos donde predominan las actuaciones situadas al margen del principio de buena fe entre Estados (bona fide) que pese a alterar notablemente la paz no cruzan los umbrales que permitirían o exigirían una respuesta armada.

Por todo lo anterior, se cree necesario dotar a los buques de guerra con sistemas que sean capaces aportar una protección extra al resto de sistemas y por ende al propio buque. Tanto es así, que se empieza a apreciar un interés por las marinas de guerra en implementar sistemas de ciberdefensa. Algunos ejemplos son las de EE.UU, Alemania, Francia y España como ya se ha comentado en la introducción. A medida que pasen los años es probable que estos sistemas sean simplemente uno más a bordo de todos los buques de guerra.

Para poder llevar a cabo el diseño del sistema de ciberdefensa se ha elegido un buque como modelo. En este caso se ha escogido la fragata F-110 que será uno de los buques que en un futuro próximo llevará este sistema instalado. En realidad, podría haber sido cualquier otro buque, pero para el autor suponía un pequeño reto al ser este el buque más moderno de la Armada que dispondrá de él.

Una vez presentados cada uno de los sistemas de la F-110, se lleva a cabo el estudio detallado de la superficie de exposición y vulnerabilidades de cada uno de ellos. Todo ello, como se ha comentado en el párrafo anterior de un modo genérico. Cabe destacar el empleo en alguno de ellos de hardware y software comercial. Esto unido a la interconexión de sistemas y la posibilidad de conexión de Internet hace que la superficie de exposición a los ciberataques se amplie. El hecho de que un sistema sea infectado podría en un momento dado permitir la libertad de movimiento a través de las distintas redes a un ciberatacante.

Finalmente, se hace mención de las ya conocidas debilidades de algunos sistemas que ya han sido hackeados como son los AIS o los sistemas de comunicaciones satélite comerciales.

2.1. Requisitos del sistema de ciberdefensa

Lo expuesto anteriormente no hace más que reforzar la idea de la necesidad de implementar un sistema a bordo de los buques que sea capaz de **identificar, proteger, detectar, responder y recuperar** los sistemas en caso de ser ciberatacados, incorporando para ello un diseño y procedimientos que lo haga ciber resiliente.

El sistema de ciberdefensa que se propone para la F-110 deberá reunir principalmente las siguientes funcionalidades: defensa en profundidad de los sistemas (protección), monitorización de eventos de ciberseguridad (detección). Dado que lo que buscamos es un sistema ciber resiliente deberíamos implementar las funcionalidades de respuesta y recuperación de este. Adicionalmente es interesante contar con una conexión de nuestro sistema con el Centro Operativo de Ciberseguridad (COCS) de la Armada y/o del Ministerio de Defensa que proporcione una monitorización remota.

Figura 1. Requisitos del sistema de ciberdefensa

2.1.1. Defensa en profundidad

La estrategia de defensa en profundidad consiste en introducir múltiples capas de seguridad o barreras que permitan reducir la probabilidad de compromiso en caso de que una de estas falle y en el peor de los casos minimizar el impacto.

El objetivo final es la protección de los sistemas, de sus activos y por ende de la información alojada en ellos.

En este apartado se analiza cada uno de los dispositivos a emplear en cada uno de los sistemas a defender del buque y que por tanto formarán parte del sistema de ciberdefensa. Entre ellos, podemos incluir como no puede ser de otra manera los cortafuegos, diodos de datos, IDS[5] e IPS[6], así como configuraciones de DMZ[7] o pasarela de intercambio de datos, sin olvidarnos de protección en los hosts con el empleo de HIDS[8] o EDR[9].

2.1.2. *Monitorización*

El sistema permitirá realizar la monitorización de todos los sistemas que integra la F-110. Esto lo llevaremos a cabo a través del ya mencionado anteriormente SIEM[10] basado principalmente en las soluciones propuestas y a lo establecido en las guías del Centro Criptológico Nacional (CCN).

2.1.3. Monitorización desde el COCS de Armada/MDEF

Por diferentes razones puede ser interesante contemplar que desde un COCS remoto, bien sea el COCS Armada o bien desde el COCS MDEF del Mando Conjunto de Ciberespacio (MCCE), se pueda

[5] Sistema de Identificación de Intrusiones
[6] Sistema de Protección de Intrusiones
[7] Zona desmilitarizada: es una red aislada que se encuentra dentro de la red interna.
[8] Sistema de Identificación de Intrusiones basado en host.
[9] Endpoint Detection and Response: son herramientas o soluciones de protección que suplen las carencias de un antivirus tradicional. Proporciona una visibilidad profunda, herramientas de investigación sencillas y opciones de respuestas automatizadas para no solo detectar la amenaza, sino para revelar su alcance y orígenes completos y responder al instante, evitando las interrupciones del negocio
[10] Sistemas de gestión de información y eventos de seguridad.

visualizar o monitorizar el estado de las redes y sistemas de los buques que se encuentran principalmente en zona de operaciones, pero también desde luego de los que se encuentran en puerto base. Esto permitirá por ejemplo en un momento dado poder emplear recursos humanos en el buque para otros puestos en una situación de mayor complejidad o estrés en zona de operaciones, al mismo tiempo que desde remoto se está llevando a cabo esta monitorización de todos los sistemas.

2.1.4. Gestión de ciberincidentes

El sistema de ciberdefensa de contar con una herramienta que permita realizar una gestión de los ciberincidentes de forma eficaz que ocurren en cada una de las redes y sistemas del buque. Para ello, debe permitir el acceso a la información de los registros recogidos en los SIEM, para poder realizar la notificación con empleo de un lenguaje común[11] en cuanto a la clasificación de ciberincidentes, niveles de amenaza y trazabilidad de estos.

2.1.5. Requisitos del personal. Personal cualificado

Todos los requisitos tecnológicos expuestos anteriormente para el sistema no servirán si no lo dotamos con el personal cualificado y la formación adecuada en esta materia.

El personal formado por la Armada en las TIC no contempla una formación específica en ciberdefensa. Por tanto, debe existir una plantilla específica en la F-110 para desempeñar estas funciones. Existe una formación en esta materia dentro del ámbito conjunto de la Fuerzas Armadas que cubre en parte los conocimientos teóricos y técnicos que debe adquirir este personal. Aun así, esta debe ser complementada con otros cursos específicos desarrollados por otras organizaciones e instituciones como son los del CCN-CERT o el instituto SANS que proporcionarán la formación requerida a los operadores del sistema.

Finalmente se plantea un sistema básico de ciberdefensa que contempla todas las particularidades de cada uno de los sistemas a defender. Para el diseño se ha querido diferenciar entre aquellos sistemas a defender que manejan información clasificada y los que no, así también atendiendo al tipo de información que maneja cada uno de ellos. Esto tiene relevancia, ya que el sistema de ciberdefensa propuesto en realidad constará de dos subsistemas. El objetivo final es no interconectar el sistema de ciberdefensa no clasificado al que sí lo es, aunque luego se pueda plasmar toda la información disponible para el analista en un mismo panel.

3. Conclusiones

Ha quedado constancia de la necesidad de contar en los buques de guerra con un sistema de ciberdefensa que le permita saber en cada momento el estado de las redes y sistemas empleados a bordo y que les permiten realizar su misión. El conocimiento de ello puede en un momento dado prevenir daños mayores en los sistemas, evitar accidentes y facilitar el desarrollo de las operaciones navales, además de mantener en todo momento informado y asesorado al Comandante del buque y mandos superiores en la cadena orgánica y operativa en lo relativo a esta materia.

[11] LUCIA se basa en la guía CCN-STIC 817 del CCN-CERT para la gestión de ciberincidentes

La cada vez mayor capacidad de los diferentes actores en el ciberespacio, el aumento de recursos tanto humanos como económicos, la mejora de conocimientos y el avance en las TTP, la creación de nuevas ciberarmas, la mayor capacidad de algunos Estados este ámbito, la financiación del algunos Estados a "proxies" sumado a la difícil atribución de las acciones en el ciberespacio, evidencia la tendencia progresiva hacia un incremento de amenazas y estrategias no convencionales e híbridas, y hacia una actuación cada vez mayor en la "zona gris" de nuestros potenciales adversarios.

Durante las últimas décadas se han producido ciberataques en el sector marítimo, no solo a navieras sino también a buques, incluidos a buques de guerra.

El empleo de tecnología COTS, y algunos casos de software obsoleto y fuera de soporte, pone más fácil al adversario el empleo de sus ciberarmas.

Se ha querido hacer un diseño de modo que la detección pueda realizarse de forma duplicada, tanto desde el COCS del buque como el de Armada o el del Mando Conjunto del Ciberespacio en tierra. Eso permitiría que desde los Cuarteles Generales que se tuviese la información del estado de los sistemas casi en "tiempo real".

No se ha querido mezclar dominios de seguridad. El hecho de interconectar los dominios supondría aumentar la superficie de exposición de los sistemas que necesitan la mayor protección posible o que manejan información clasificada, y por tanto hacerlos más vulnerables.

De este modo, aunque supone tener el doble de elementos, SIEM y puestos de operador, se considera conveniente que no exista interconexión entre ambos dominios.

Aun así, todo lo anterior, no tiene sentido si no se dispone un personal cualificado y específicamente forma en la materia de ciberdefensa. Por lo tanto, se considera imprescindible que, para poder tener un sistema completo, no solo el recurso material adecuado sino un recurso humano de calidad.

Referencias

[1] "Independent - Keith Martin Rory Hopcraft". (Jun. 2018). "50,000 Ships worldwide are vulnerable to cyberattacks.".

[2] "Kaspersky - Kate Kochetkova". (May 2015). "Maritime industry is easy meat for cyber criminals".

[3] "BBC" (Mar 2022). "Russia hacked Ukrainian satellite communications, officials believe [En línea]. Available: https://www.bbc.com/news/technology-60796079.

[4] Navantia Notas de prensa. Navantia y Telefónica Tech instalarán un sistema de ciberseguridad reforzado en los submarinos de la clase S-80. (30 de noviembre de 2021).

[5] Bob Freeman. Press Release US Navy. A New Defense for Navy Ships: Protection from Cyber Attacks (18 de septiembre de 2015).

[6] Jaime Karremann. Cyber security at sea, defending against digital attacks on ships. (29 de septiembre de 2021).

[7] Naval Group launches the first defense and intervention frigate (FDI) for the French Navy. Revista EDR online. (7 de noviembre de 2022).