Sistema de ciberinteligencia en apoyo a los procesos de decisión en la Armada: concepto y metodología

Autor: Mesa Fernández, Juan Pablo

Director: Rodríguez Rodríguez, Francisco Javier

Contacto: jmesfer@fn.mde.es

Resumen: En los últimos años, la aparición de los asuntos del ciberespacio habría obligado a los ejércitos y otras organizaciones a adaptarse a un nuevo entorno operativo aún más complejo e incierto para lograr sus objetivos. Entender sus retos y oportunidades es un aspecto clave para la correcta toma de decisiones.

Las capacidades de ciberdefensa en la Armada están en continua adaptación y crecimiento para responder a esta situación. Sin embargo, en este trabajo se ha identificado la necesidad de cerrar un vacío en el ámbito de la inteligencia, desde la argumentación de que un sistema de mando y control robusto nace desde la mejor comprensión del entorno incluyendo su componente de ciberespacio, por lo que necesita un sistema de ciberinteligencia propio que se la proporcione.

Si bien el nivel estratégico y operacional habrían reaccionado a esta circunstancia, en los niveles de conducción táctico y en las estructuras orgánicas de los ejércitos y de la Armada no habría permeado aún la importancia e influencia de la ciberintegencia; obviando así riesgos, retos, oportunidades y amenazas y comprometiendo con esta situación la propia misión. Éste es el caso de la escasa integración de los asuntos del ciberespacio en el planeamiento y conducción de operaciones navales; o, desde un punto de vista orgánico, el sesgo que se produce en los procesos de adquisición de capacidades con tecnologías disruptivas como el Big Data, la Inteligencia Artificial o 5G, que en la búsqueda de la superioridad de la información, podría olvidar la seguridad por diseño al no contar con estructuras especializadas que planteen los riesgos asociados al ciberentorno.

En este contexto, el presente TFM propone la generación de una nueva capacidad militar que integre el entendimiento de lo ciber en los procesos de decisión de la Armada, tanto en su actividad orgánica como en la operativa. Se definen, así, los conceptos de empleo, organización, formación, relación con otros entes y también la metodología de apoyo a la decisión, explicada a través de un caso práctico.

Palabras clave: Ciberinteligencia, Ciberespacio, Ciberdefensa, Entorno marítimo, Ciberamenazas, Inteligencia, Mando y Control, Decisión.

---

1. Introducción

1.1. Motivación y planteamiento del problema

Este trabajo pretende subrayar la necesidad de generar un sistema de cibertinteligencia como capacidad imprescindible para la toma de decisiones, proponiendo un modelo para la estructura de la Armada. Es un aspecto en el que la comunidad militar aún no ha delimitado siquiera su propia definición, alcance, procesos o responsabilidades.

El problema radica en que, a pesar de que en los últimos años el ciberespacio se haya erigido como un nuevo entorno de actuación, los ejércitos estarían aún en proceso de adaptación y no poseerían la capacidad ni la cultura operacional de considerar adecuadamente la influencia del ciberentorno sobre su actividad.

La situación actual reside en que el conocimiento de lo que ocurre, o bien se obvia, o bien se trata con medios y disciplinas tradicionales que no responden a los retos actuales. En el mejor de los casos, el estudio del ciberespacio se gestiona con capacidades retenidas a muy alto nivel de conducción, a menudo duplicando esfuerzos y sin una clara línea de responsabilidad entre las partes que tienen interés. Como consecuencia, el sistema actual es poco eficiente y ágil para responder a los retos a los que se enfrenta el decisor de la Armada.

1.2. Objetivos

El objetivo principal del presente trabajo reside en presentar una propuesta de capacidad de ciberinteligencia en la estructura de la Armada que le permita mejorar sus procesos de decisión para hacer frente a los retos y oportunidades del entorno cibermarítimo.

Para ello, se analiza cómo la irrupción de los asuntos del ciberespacio influye en la actividad y misiones de la Armada y condiciona el ejercicio del mando, siendo necesario integrar un sistema de ciberinteligencia para mejorar el proceso de decisión. Confirmando la hipótesis anterior, se define a continuación un concepto de empleo del sistema de ciberinteligencia de la Armada y se esboza la composición de la unidad que proporcionaría tal capacidad, estableciendo sus funciones, cometidos, relaciones y beneficios. Para finalizar, se realiza una descripción de algunos procesos de mando y control en los que la ciberinteligencia podría aportar valor.

2. La Armada y el entorno cibermarítimo

La irrupción del ciberespacio no cambia la filosofía de mando y control, si bien introduce nuevos retos que obligan a los ejércitos a adaptar sus estructuras y procedimientos [1]. El entorno marítimo no es ajeno a tales cambios y sus condicionantes repercuten en la actividad de la Armada afectando todo el rango de operaciones navales: desde la seguridad y el conocimiento del entorno marítimo, a la disuasión o el enfrentamiento armado con un adversario híbrido o convencional [2] [3].

En este contexto, la capacidad de ciberinteligencia se identifica como clave en los procesos de decisión. La famosa niebla de la guerra se hace aún mayor con la inclusión de este nuevo dominio, idóneo para un adversario de estrategia híbrida o de zona gris que pretenda explotar nuestra dependencia de los sistemas CIS/TIC. No entender o identificar estas dinámicas significa ceder el

terreno clave del ciberespacio, tan necesario para el empleo de sistemas TI/TO o la propia toma de decisiones.

Los decisores de la Armada no pueden ni deben renunciar a un sistema de inteligencia completo y propio. Este sistema, necesariamente, debe contemplar la perspectiva ciber para identificar no sólo adversarios, capacidades o sus intenciones, sino también las oportunidades que este dominio puede ofrecer. La responsabilidad de dibujar el umbral del riesgo es del decisor, que poco podrá hacer si no posee la capacidad que lo vislumbre.

La estructura actual de la Armada no proporciona la mencionada capacidad. Su nuevo *Concepto de Empleo de Ciberdefensa* [4] implícitamente asume el riesgo desde la argumentación de que el nivel táctico o la estructura de los ejércitos no son el nivel apropiado para introducir las capacidades de ciberinteligencia, pues ya se llevan a cabo en el MCCE y CIFAS. Sin embargo, un sistema propio mejora los principios de inteligencia sin repercutir en el control centralizado en el nivel superior. Una capacidad propia en la Armada cierra el círculo, engranando los mecanismos de decisión de nivel táctico y mejorando la capacidad de respuesta al situarse en una posición de privilegio entre el decisor marítimo y la relación funcional con estructuras de nivel superior, como MCCE y CIFAS.

3. Definición, alcance y concepto de empleo de la capacidad de ciberinteligencia en la Armada

Este capítulo se centra en proponer un concepto y metodología de un sistema de ciberinteigencia propio que posibilite afrontar los retos del entorno donde la Armada desarrolla su actividad. Está basado en las mismas prácticas, principios doctrinales y filosofías de mando y control e inteligencia, ahora sí, haciéndolos extensivos al estudio del ciberespacio. [5-8]

A falta de una definición consensuada de ciberinteligencia, a los efectos de este trabajo se definiría como aquella *capacidad militar que con un enfoque en el ciberespacio y que de manera continuada y coordinada con el ciclo de inteligencia, contribuye al entendimiento del entorno cibermarítimo contribuyendo a la mejora de los procesos de decisión, el mejor empleo de capacidades navales y/o el mantenimiento de la libertad de acción en el ciberespacio asociado*.

Así, la capacidad inicial de ciberinteligencia se visualiza organizativamente en el Grupo de Ciberdefensa de la Armada (GRUCIBER) y con relación funcional con el sistema de inteligencia. Es un modelo centralizado y desplegable, como estrategia más eficiente a corto y medio plazo, ante la dificultad de formar un equipo de analistas especializados en el campo de la ciberdefensa, inteligencia y operaciones navales.

El beneficio se identifica en tres diferentes dimensiones de toma de decisión:

a) Dimensión táctico-técnica, con la generación de *Inteligencia de Ciberamenazas* (CTI) en apoyo a la ciberdefensa de los sistemas que la Armada tiene asignados en su zona de responsabilidad. Su fortaleza reside en la federación de fuentes de inteligencia y la automatización de la seguridad y defensa de redes y sistemas (*Security Orchestration, Automation and Response*, SOAR).

b) Dimensión de las operaciones navales, mediante la integración en los procesos de planeamiento y conducción de las operaciones. Este ámbito, por ser el más demandante y razón de ser de la Armada ha sido el elegido para profundizar en la metodología de integración de ciberinteligencia mediante un caso de estudio. La actualización del *Cyber Situational Awareness* (CySA), el *Cyber Intelligence*

Preparation of the Operational Environment (CyIPOE), Análisis de CoG para *Targeting* e Influencia, valoración de las operaciones,..etc. son algunas metodologías presentadas.

c) Dimensión estratégica, proporcionando apoyo de inteligencia estratégica al SIFAS y asesoramiento a la alta dirección en sus procesos de trabajo relacionados la actividad orgánica de la Armada. En este sentido, es especialmente interesante el beneficio de contar con un equipo de analistas de ciberinteligencia para la adquisición de nuevas tecnologías emergentes y disruptivas (5G, inteligencia artificial, etc…) y conseguir que la Armada, en plena transformación digital, obtenga superioridad tecnológica y de la información bajo el principio de seguridad por diseño.

Figura 1. Ciclo de ciberinteligencia y su contribución al nivel de decisión. (Elaboración propia)

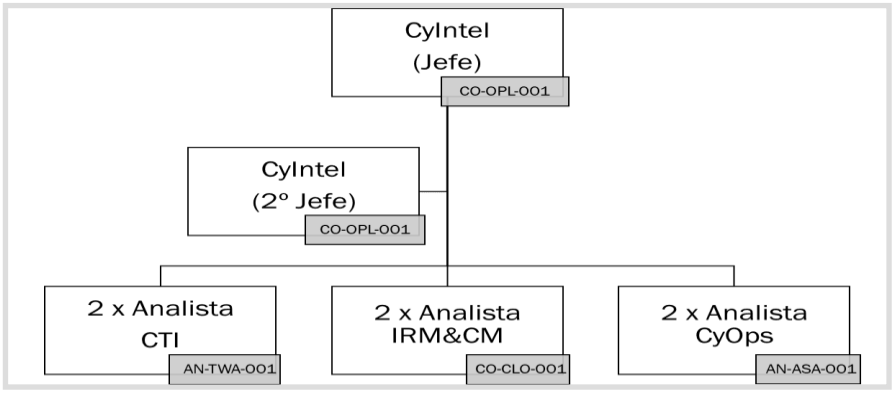

Figura 2. Propuesta de organización de unidad de ciberinteligencia de la Armada (Elaboración propia a partir de [9]).

El sistema de ciberinteligencia se ha diseñado en torno a un núcleo inicial compuesto por ocho miembros con una formación multidisciplinar. Sus perfiles profesionales se han diseñado a partir de competencias que incluyen desde las tradicionales técnicas de inteligencia y planeamiento de operaciones e influencia, hasta conocimientos técnicos de operaciones de ciberdefensa, análisis de sistemas e ingeniería inversa. Para configurar el perfil profesional de cada puesto de trabajo se ha recurrido a un marco del *National Initiative for Cybersecurity Education* (NICE) [9], elaborando una detallada descripción de sus funciones, destrezas, conocimientos y habilidades.

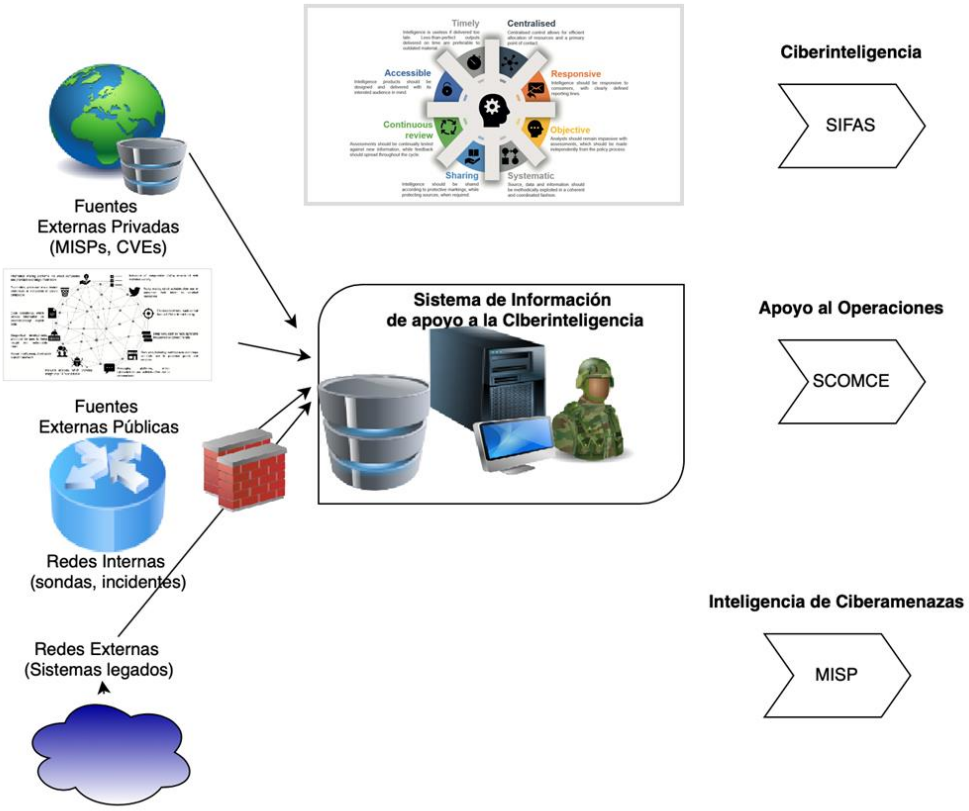

Figura 3. Sistema de Información en Apoyo a la Ciberinteligencia de la Armada (SIaCI) (Elaboración propia)

La capacidad diseñada contempla el empleo de un sistema de información de apoyo a la Ciberinteligencia (SIaCI) que, basado en una filosofía de transformación digital, explota de manera sistemática las fuentes de interés y la información de los sistemas legados a los que está federado, facilitando las actividades del ciclo de ciberinteligencia de un manera particularizada para cada nivel de decisión.

4. Conclusiones

El desarrollo del trabajo abordado permite considerar que se han alcanzado y demostrado los objetivos planteados para este TFM, cuya argumentación se resume en los siguientes puntos:

La irrupción del ciberespacio no cambia la filosofía de mando y control, si bien introduce nuevos retos que obligan a los ejércitos a adaptar sus estructuras y procedimientos. En la Armada, esa adaptación se identifica en la conveniencia de establecer una estructura orientada a extender la actividad de la inteligencia hasta el campo de la ciberdefensa, y viceversa, solapando dos ámbitos que aún no han establecido relación conjunta.

La constitución e integración de un sistema de ciberinteligencia en la estructura de la Armada mejora sus procesos de decisión. La clave del éxito se identifica en la capacidad de entendimiento, enlace y aprovechamiento de las capacidades ciber y de inteligencia, residentes en niveles superiores,

y su orientación a las necesidades del decisor para satisfacer las necesidades de su sistema de decisión con los condicionantes que incorpora el ciberespacio. Esta capacidad inicialmente se origina a través de la constitución de una unidad de ciberinteligencia con carácter centralizado aunque desplegable y formación multidisciplinar.

El segundo pilar de éxito se ha identificado en el sistema de información en el que se apoya. Se ha presentado la arquitectura de referencia del SIaCI como *hub* generador de apoyo a los procesos de decisión en cada dimensión mediante una metodología de integración de ciberinteligencia.

Agradecimientos

A mis compañeros de Máster, por hacer de esta etapa una experiencia fantástica que me ha permitido conocer a grandes profesionales y mejores personas.

Referencias

1. Jefe de Estado Mayor de la Defensa, Concepto de empleo de Ciberdefensa 2018.
2. J. Jordán, *Una oscura 'zona gris'* [En línea]. Disponible en: https://global-strategy.org/una-oscura-zona-gris/ [Último acceso: octubre 2022].
3. Gobierno de España, *Estrategia de Seguridad Nacional 2021 [En línea]*. *Disponible en:* https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017 [Último acceso: octubre 2022].
4. Concepto de Empleo de Ciberdefensa de la Armada 2022.
5. U.S. Marine Corps, *MCDP 1 Warfighting*, Department of the Navy, Headquarters United States Marine Corps, 1997.
6. EMAD, *PDC 3-20. Doctrina de Operaciones en el Ámbito Ciberespacial, 2021*.
7. EMAD, *PDC-01(a) Doctrina para el empleo de las Fuerzas Armadas*, 2018.
8. OTAN, *AJP-2 Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*, NATO Standardization Agency, 2020.
9. «Web de NIST» [En línea], Disponible en: https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final; [Último acceso: noviembre 2022].