B.OTN

BOLETÍN DEL OBSERVATORIO DE TÁCTICA NAVAL

ESOA

“Defensa Antimisiles: estudios matemáticos” Pág. 05

FadARA
Facultad de la Armada

MAYO
2025

» Autoridades

Director General de Educación de la Armada

CL Lic. Contralmirante Juan Carlos Romay

Decano de la Facultad de la Armada

CL (RE) VGM Mg. Ing. Juan Carlos Bazán

Director de la Escuela de Oficiales de la Armada
CN Lic. Darío Andrés Buscarolo

Secretario de Extensión de la Escuela de Oficiales de la Armada
CN (RE) Abog. Guillermo Martínez

» Equipo Editorial

Director del Observatorio
CN (RE) Prof. Lic. Guillermo Spinelli

Coordinador de Temáticas
CF Sebastián Campi

Responsable del Boletín
Prof. Mg. Eugenio Koutsovitis

Contenido

» Bienvenidos

Por Prof. Mg. Eugenio Koutsovitis [1]

Con gran satisfacción presentamos el **tercer volumen del Boletín del Observatorio de Táctica Naval**, una publicación que busca consolidarse como espacio de reflexión, análisis e intercambio en torno a la práctica táctica naval, sus fundamentos doctrinarios, y las transformaciones tecnológicas y estratégicas del presente.

En esta edición, continuamos con el propósito de articular el estudio riguroso de casos históricos con los desafíos operativos contemporáneos. La combinación de enfoques técnicos, analíticos e históricos que aquí se despliega refleja tanto la riqueza del campo como el compromiso del Observatorio con una mirada crítica, profesional y actualizada.

La Guerra en Ucrania, el impacto de los sistemas no tripulados, el radar como hito tecnológico, el concepto de centro de gravedad en el pensamiento militar, y la reevaluación de batallas icónicas como Jutlandia son solo algunas de las aristas que este número aborda, siempre con la convicción de que el conocimiento táctico no es sólo pasado, sino herramienta vital para pensar el presente y proyectar el futuro.

Agradecemos a todos quienes aportaron a esta edición, y renovamos la invitación a investigadores, docentes, oficiales y estudiantes a **enviar contribuciones** para futuros volúmenes. Sabemos que la táctica naval no se piensa en soledad: se construye, se debate y se transmite colectivamente.

Bienvenidos a bordo.

[1] Responsable editorial del Boletín del Observatorio de Táctica Naval. Profesor y licenciado en Ciencia Política (UBA), Magíster en Defensa Nacional (UNDEF), Docente en la Carrera de Ciencia Política (UBA), Maestrando en Administración Pública (USAL). Subsecretario de Relaciones Institucionales y Vinculación Universitaria de la Facultad de la Armada.

» Defensa Antimisil I

Por CN (RE) Prof. Lic. Guillermo Spinelli [2]

A continuación se detallan varios incidentes históricos, desde la Segunda Guerra Mundial hasta la actualidad, en los que buques de superficie enfrentaron ataques con misiles antibuque. En cada caso se indican el año, conflicto, tipo de buque, misil atacante (con velocidad y perfil de vuelo), características del radar o sistema de detección del buque, la distancia estimada a la que se detectó (o no se detectó) el misil y el resultado del ataque. Cabe aclarar que la información es escaza y en algunos casos contradictoria.

Casos Históricos Seleccionados de Defensa de Buques contra Ataques de Misiles

1943 – Hundimiento del acorazado *Roma* (Segunda Guerra Mundial)

- **Conflicto y buque:** Segunda Guerra Mundial; *Roma* era un acorazado italiano moderno (clase Vittorio Veneto) y buque insignia de la Regia Marina italiana.
- **Misil utilizado:** Bomba guiada alemana Ruhrstahl*Fritz X* (FX-1400). Aunque técnicamente era una bomba planeadora radio-dirigida (no autopropulsada), fue la primera arma guiada antibuque empleada en combate. Se lanzaba desde bombarderos a gran altitud (≈6.000 m) para ganar energía potencial. Su velocidad de caída superaba los 300 m/s (más de 1000 km/h) en el tramo final, prácticamente vertical, y estaba diseñada para perforar cubiertas blindadas.
- **Perfil de detección del buque:** *Roma* disponía de radares de alerta aérea de la época (radar EC-3 ter "Gufo") para detectar aviones enemigos. En 1943 estos sistemas podían avistar bombarderos aéreos a decenas de kilómetros. Sin embargo, no estaban concebidos para rastrear bombas individuales una vez desprendidas. La táctica alemana era lanzar el *Fritz X* fuera del alcance de la artillería antiaérea, desde ~6 km de altitud. Esto brindaba a la tripulación de *Roma* aviso de la presencia de aviones enemigos, pero no de la bomba guiada en descenso. De hecho, la *Fritz X* caía casi verticalmente, dificultando su observación visual hasta instantes antes del impacto.

[2] Capitán de Navío (RE), profesor y licenciado en historia. Secretario de Extensión y Vinculación Universitaria de la Facultad de la Armada (FadARA).

- **Distancia de detección del misil:** No se conocen datos de detección del misil como tal – el *Roma* detectó los bombarderos Do-217 pero no distinguió la bomba en el aire. En la práctica, la tripulación no tuvo alerta específica de la *Fritz X*. Solo cuando impactó se supo del ataque. La bomba golpeó *Roma* a las 15:45 del 9 de septiembre de 1943. Minutos después un segundo *Fritz X* alcanzó el buque, provocando una explosión catastrófica en el pañol de municiones que hundió al acorazado en media hora.

- **Resultado del ataque:** el acorazado*Roma* sufrió dos impactos directos y se hundió rápidamente, llevándose la vida de ~1.300 marinos. Este ataque supuso la primera baja de un buque capital por un arma guiada. La sorpresa tecnológica fue grande: los italianos no tenían contramedidas. Posteriormente, los Aliados desarrollaron contramedidas de guerra electrónica (interferidores de radio) para contrarrestar las *Fritz X*, reduciendo mucho su eficacia.

Comentarios Estrictamente, la *Fritz X* era una bomba planeadora, no un misil crucero, pero se la incluye por ser precursora de los misiles antibuque modernos. Este caso muestra que en 1943 los buques dependían de detectar los aviones lanzadores, no las municiones en sí – una limitación significativa ante la nueva amenaza.

1967 – Ataque al destructor *INS Eilat* (Posguerra de los Seis Días)

- **Conflicto y buque:** Guerra de Desgaste (tensión tras la Guerra de los Seis Días); *INS Eilat* era un destructor israelí (ex-HMS *Zealous*, clase Z británica de la SGM) de 2.530 ton, con artillería convencional. Patrullaba internacionalmente frente a Port Said (Mediterráneo).

- **Misil utilizado:** Misil antibuque soviético *P-15 Termit* (OTAN: SS-N-2 *Styx*), lanzado desde lanchas rápidas egipcias clase Komar. El *Styx* es un misil de crucero subsónico (≈Mach 0,8–0,9), con alcance ~40 km y un perfil de vuelo relativamente alto en su época (vuelo de crucero a decenas de metros sobre el mar, descendiendo en fase terminal). Tenía un motor cohete de combustible líquido y un gran fogonazo al lanzamiento.

- **Perfil de detección del buque:**el destructor *Eilat* poseía radares de origen británico de los años 50/60 para búsqueda aérea/superficie, adecuados para aviones o barcos pero de efectividad limitada contra un misil pequeño a baja altura. El 21 de octubre de 1967, el *Eilat* navegaba a ~14 millas de la costa egipcia cuando dos lanchas Komar le dispararon misiles desde la protección del puerto de Port Said. Los vigías del *Eilat* avistaron un destello y humo en dirección al puerto (indicativo del lanzamiento) a las 17:16 hora local. Inicialmente se confundió con el lanzamiento de un cohete de señales, por lo que no se dio la alarma de inmediato. Segundos después, al comprender la situación, se ordenó cubrir puestos de combate y el buque inició maniobras evasivas. Los radares de *Eilat* no detectaron el *Styx* en ese primer instante – la alerta provino de observación visual.

- **Distancia de detección del misil:** El primer misil fue identificado visualmente en vuelo cuando aún parecía pasar de largo por la popa. Recién **a unas ~6 millas náuticas (≈11 km)** del buque el *Styx* viró súbitamente en busca del blanco, momento en que la tripulación confirmó la amenaza. En esa fase final, *Eilat* abrió fuego antiaéreo, pero sin éxito, ya que el misil volaba bajo y rápido. **En resumen, la detección efectiva ocurrió muy tarde, alrededor de 6 mn de distancia, y de forma visual.** No hay constancia de que el radar del *Eilat* llegara a fijar el blanco antes del impacto.

- **Resultado del ataque:** El primer *Styx* impactó en la popa de *Eilat*, causando graves daños (voló la sección de popa). Minutos después, a las 17:28, *Eilat* radiaba que había sido atacado por "aviones enemigos" y estaba averiado, reflejando la confusión táctica (se creía que el misil era una bomba lanzada por avión). Un segundo misil golpeó la sección media poco después, dejándola envuelta en llamas. Incapaz de maniobrar y gravemente dañada, la tripulación combatió incendios e inundaciones por dos horas. Alrededor de las 19:45, un **tercer misil** alcanzó al destructor, detonando pañoles y causando explosiones masivas. *Eilat* se hundió 15 minutos después del tercer impacto. Un cuarto misil fue lanzado y cayó al mar donde *Eilat* había estado, rociando a los náufragos con metralla y combustible en llamas. El ataque causó 47 muertos y más de 100 heridos entre la tripulación.

- **Comentarios:** Fue el primer hundimiento de un buque con misiles antibuque, sorprendiendo a las armadas del mundo. Investigaciones israelíes apuntaron a complacencia operacional, pese a saber que Egipto poseía misiles *Styx*, el *Eilat* patrullaba sin cobertura aérea cercana y con confianza excesiva La detección dependió de vigías en lugar de instrumentos, evidencia de que los sistemas de alerta de la época no estaban preparados para misiles de bajo vuelo. Tras el incidente, muchas armadas aceleraron la adopción de contramedidas electrónicas y tácticas evasivas frente a misiles antibuque

.

1971 – Destrucción del *PNS Khaibar* (Guerra Indo-Pakistaní de 1971)

- **Conflicto y buque:** Guerra Indo-Pakistaní de 1971; *PNS Khaibar* era un destructor pakistaní clase *Battle* (ex-HMS *Cádiz*, desplazamiento ~3.600 ton), veterano de la SGM. Patrullaba cerca de Karachi durante el conflicto.

- **Misil utilizado:** Misil antibuque *P-15 Termit* (SS-N-2 *Styx*) de fabricación soviética, lanzado por la armada india. La noche del 4 de diciembre de 1971, lanchas misilísticas indias clase Vidyut (proyecto 205, versión de exportación de las Osa soviéticas) atacaron Karachi en la **Operación Trident**, disparando varios *Styx*. *INS Nirghat* lanzó el primer *Styx* contra *Khaibar* a unos ~20–25 km

. El *Styx*, subsónico y con un perfil de vuelo relativamente alto en esa versión inicial, se aproximó al destructor en la oscuridad de la noche (alrededor de las 22:45 hora local).

- **Perfil de detección del buque:** *Khaibar* estaba en estado de alerta debido a la guerra, pero es posible que esperara ataques aéreos más que misiles mar-mar. El destructor disponía de radar de vigilancia aérea y de superficie de los 60s. Según reportes, *Khaibar* **detectó algo en el radar entrante y asumió que era una aeronave enemiga**, dado que los misiles eran un fenómeno nuevo. El buque activó sus baterías antiaéreas, disparando contra el supuesto "avión" atacante. Esta reacción indica que *Khaibar* detectó el *Styx* (o su llama) lo suficientemente lejos para intentar responder, aunque de forma incorrecta al confundir la naturaleza del blanco. Posiblemente el destello del misil o un eco de radar sin identificación (sin transpondedor IFF) fue interpretado como un avión a baja altitud

- **Distancia de detección del misil:** No hay datos públicos exactos, pero la secuencia sugiere una detección tardía. El lanzamiento ocurrió a ~13–15 mn de distancia; *Khaibar* aparentemente solo reaccionó en el último minuto, cuando el misil ya estaba próximo. De hecho, el mensaje de auxilio de *Khaibar* enviado tras el impacto decía "**avión enemigo atacó en posición… caldera No.1 alcanzada, buque parado**", mostrando que no identificaron un misil hasta después del daño. Es probable que el *Styx* se detectara (visualmente o por radar) dentro de los últimos ~5–10 km, demasiado tarde para una defensa eficaz.

- **Resultado del ataque:** El primer *Styx* impactó en el costado de estribor de *Khaibar*, explotando bajo el comedor de marinería a las 22:45. Provocó la explosión de la primera sala de calderas y dejó el buque sin propulsión ni electricidad. Al ver que seguía a flote, la lancha *Nirghat* lanzó un segundo *Styx* que golpeó la segunda sala de calderas, hundiendo finalmente al destructor y matando a 222 tripulantes La mayoría de la dotación se fue a pique con el buque. Este ataque simultáneo hundió también a otro buque paquistaní (el barreminas *PNS Muhafiz*) con un *Styx*, y dañó gravemente al destructor *PNS ShahJahan*.

- **Comentarios:** La **Operación Trident** demostró la letalidad de los misiles antibuque en combate nocturno. El*Khaibar* no pudo defenderse eficazmente: sus armas antiaéreas eran inútiles contra un misil tan rápido y de vuelo bajo. La confusión táctica (creer que era un avión) muestra la sorpresa de la época – los paquistaníes no habían entrenado para este tipo de ataque. Este caso reforzó la importancia de los sistemas de alerta temprana específicos para misiles y de la guerra electrónica. Se destaca que la detección fue insuficiente, incluso con radares relativamente modernos, un misil *Styx* entrante a baja altura resultó prácticamente una sorpresa táctica.

1982 – Ataque al destructor *HMS Sheffield* (Guerra de las Malvinas)

- **Conflicto y buque:** Guerra de las Malvinas (1982); el *HMS Sheffield* era un destructor británico Tipo 42 (3.600 ton) equipado con misiles antiaéreos Sea Dart. Servía de piquete de radar en la TaskForce británica.

- **Misil utilizado:** Misil antibuque francés *AM39 Éxocet*, lanzado por aviones argentinos Super Étendard. El Éxocet es un misil crucero subsónico (≈Mach 0,93), con alcance ~50–70 km en versión aire-superficie, dependiendo de la altura y velocidad de lanzamiento. Su rasgo más peligroso es el **vuelo rasante al mar (sea-skimming)**: en aproximación final vuela a **2–5 metros** sobre la superficie, ocultándose bajo el horizonte radar hasta unos pocos kilómetros del blanco. Posee un buscador radar activo en banda I para la fase terminal. En el ataque del 4 de mayo de 1982 contra el *Sheffield*, dos Éxocet fueron lanzados a ~30–40 km de distancia.

- **Perfil de detección del buque:**el destructor *Sheffield* disponía de un radar de búsqueda aérea de largo alcance (Tipo 965M) y radares de control de tiro 909 para sus misiles Sea Dart, Ambos radares tenían muchas limitaciones contra blancos volando a baja altura. También contaba con receptores de alerta radar (ESM) UAA-1, para detectar emisiones radar enemigas. Carecía de **un sistema activo de contramedidas electrónicas (ECM) ni CIWS cercano**, y su estado de alerta antiaérea era bajo en ese momento. Antes del ataque, el *Sheffield* había evaluado que la amenaza Éxocet estaba "sobrevalorada" y relajó su vigilancia. La sección de comunicaciones satelitales estaba transmitiendo, lo que bloqueó temporalmente el receptor de alerta UAA-1 del buque. Por tanto, el buque no recibió la advertencia que otro destructor (HMS *Glasgow*) había emitido sobre contactos aéreos enemigos.

- **Distancia de detección del misil:** Extremadamente corta. *No* **detectó por radar los Éxocet entrantes** – venían bajo el horizonte y su tripulación no estaba en alerta máxima. No hubo tiempo de lanzar misiles Sea Dart ni contramedidas de ningún tipo. **La primera indicación fue visual:** marinos en cubierta avistaron *humo en el horizonte acercándose*, gritaron "¡misil en acercamiento!" segundos antes del impacto. Es decir, se identificó el rastro de humo del Éxocet **a escasos segundos/metros**, quizá a ~2 km o menos. En ese momento era demasiado tarde para reaccionar. Según informes oficiales, el *Sheffield* literalmente no vio venir el misil hasta que golpeó (el capitán ni siquiera fue llamado al puente antes del impacto). Un segundo Éxocet lanzado simultáneamente pasó de largo (fue avistado por otro buque, HMS *Yarmouth*, y cayó al mar 0,5 mn más allá). Esto confirma que los misiles *no* aparecieron en los radares del destructor ni hubo alerta temprana.

- **Resultado del ataque:** A las 11:04, el Éxocet impactó en el costado de estribor, a la altura de la línea de flotación, penetrando el casco. La cabeza explosiva de 165 kg no detonó propiamente, pero el combustible de cohete provocó un incendio masivo e incontrolable. El buque quedó sin energía eléctrica ni capacidad de combate. Tras horas de lucha contra el fuego, *el* destructor fue evacuado y se hundió seis días después mientras era remolcado, en el ataque fallecieron 20 marinos.

- **Comentarios:** La pérdida de *Sheffield* evidenció el peligro de los misiles rasantes y algunos fallos: la falta de alerta temprana (ignoró advertencias previas creyéndolas falsas alarmas), problemas de entrenamiento en distinguir blancos (Mirage vs Étendard) en el radar, e incluso obstrucción del ESM por uso de radio erróneo. El caso generó importantes investigaciones desclasificadas años más tarde, que confirmaron el impacto del Éxocet y las deficiencias en la respuesta. A corto plazo, la Royal Navy adoptó contramedidas improvisadas (chaff) y aumentó la alerta. En perspectiva, *Sheffield* mostró que un misil pequeño y rápido puede eludir los sensores tradicionales, subrayando la necesidad de radares de baja cota 3D y sistemas CIWS, adoptados posteriormente.

1987 – Ataque al *USS Stark* (Guerra Irán-Irak)

- **Conflicto y buque:** Guerra Irán-Irak (en plena "guerra de los petroleros" en el Golfo Pérsico); *USS Stark* (FFG-31) era una fragata estadounidense clase Oliver Hazard Perry (despl. ~4.100 ton) con misiles antiaéreos Sparrow y sistema CIWS Phalanx. Patrullaba como neutral para proteger buques mercantes.

- **Misil utilizado:** Misil antibuque *AM39 Éxocet* francés, lanzado el 17 de mayo de 1987 por un caza iraquí Mirage F1. Se dispararon dos Éxocet desde aproximadamente **10–12 millas náuticas de distancia (≈18–22 km)**. Los misiles volaron hacia *Stark* a ~Mach 0,9 y a muy baja altitud sobre aguas calmadas. Cabe destacar que el lanzamiento se hizo desde ~5.000 pies de altitud; luego los Éxocet descienden a ras del mar para el ataque final

- **Perfil de detección del buque: la** *Stark* contaba con un radar aéreo de búsqueda AN/SPS-49 (2D) y un radar de control de tiro, además del detector radar ESM AN/SLQ-32. En teoría podía detectar amenazas aéreas a decenas de km. De hecho, rastreó al Mirage iraquí en aproximación, pero **no lo identificó como hostil**, el avión no parecía atacar (Iraq no era enemigo declarado). Por reglas de enfrentamiento de presencia neutral, *Stark* no podía abrir fuego preventivo sin clara amenaza. Respecto a los misiles, *el buque* enfrentó condiciones atmosféricas adversas para el radar: se cree que una **capa ductora de inversión térmica** en el Golfo atrapó las señales de radar cerca de la superficie, impidiendo detectar objetos a muy baja altitud. Este "canal de propagación" hizo que ni el radar de vigilancia ni el receptor SLQ-32 (montado alto en el mástil) captaran la señal del buscador del Éxocet que venía prácticamente pegado al mar. Además, la fase de alerta fue breve, los misiles tardaron ~1 minuto en llegar desde el lanzamiento (unos 10 mn de recorrido a ~10 millas por minuto).

- **Distancia de detección del misil: la** *USS Stark* **no logró detectar los misiles hasta instantes antes del impacto, y únicamente de forma visual**Según análisis posteriores, la única oportunidad clara de detección habría sido durante los ~20 segundos en que cada Éxocet descendía desde la altitud de lanzamiento (~1500 m) hasta su altura de crucero rasante. En esa ventana, en el radar del *Stark* los misiles habrían sido ecos muy pequeños y transitorios, posiblemente filtrados como ruido. De hecho, ningún arma defensiva se activó a tiempo. Solo cuando uno de los misiles se acercó mucho, algunos marinos alcanzaron a verlo y el oficial de guardia gritó "¡misil en acercamiento!" apenas unos segundos antes del impacto, sin tiempo para respuesta. **En resumen, la detección efectiva fue prácticamente nula hasta el momento del impacto**.

- **Resultado del ataque:** El primer Éxocet penetró el costado de estribor de la*Stark* y, aunque su ojiva de 165 kg no explotó, el combustible en llamas causó un gran incendio en la zona de habitabilidad. Unos 30 segundos después, el segundo Éxocet impactó casi en el mismo lugar y **detonó**, abriendo un rumbo de 3×4,5 metros en el casco. El incendio resultante arrasó los compartimentos. Murieron 37 marinos y 21 resultaron heridos. Pese al grave daño, la tripulación logró sofocar el fuego tras horas de lucha, evitando el hundimiento. La fragata quedó seriamente averiada pero permaneció a flote, siendo auxiliada y reparada posteriormente.

- **Comentarios:** La investigación reveló fallos en la postura de defensa del buque no activó su Phalanx CIWS ni lanzó chaff, en parte por la **confusión IFF/política** (no querer derribar un avión posiblemente "amigo" sin confirmación). Pero técnicamente, el principal problema fue la detección tardía debido al horizonte radar y posiblemente condiciones de refracción anómala. Este incidente subrayó la necesidad de mejorar la **detección de misiles rasantes en entornos litorales cálidos**. Tras el ataque, la US Navy ajustó sus reglas de enfrentamiento (permitiendo respuestas más agresivas ante amenazas sospechosas) y mejoró sistemas: se introdujeron alertas automatizadas del sistema SLQ-32 y tácticas para contrarrestar ductos atmosféricos. El ataque a la *Stark* mostró paralelismos con del *Sheffield* , en ambos casos, el Éxocet se acercó sin ser visto hasta el último momento pero también diferencias, la *Stark* estaba al menos rastreando al avión, aunque no supo interpretar la amenaza a tiempo.

1991 – Interceptación de misil Silkworm contra el *USS Missouri* (Guerra del Golfo)

- **Conflicto y buque:** Guerra del Golfo (Operación Tormenta del Desierto, 1991); la coalición aliado-occidental en el Golfo enfrentó ataques con misiles iraquíes. El *USS Missouri* (BB-63) era un acorazado estadounidense de la SGM modernizado, desplegado en el Golfo para misiones de bombardeo costero. Iba escoltado por buques con defensa antiaérea moderna, incluyendo el destructor británico *HMS Gloucester* (Tipo 42).

- **Misil utilizado:** Misil antibuque chino *HY-2 Silkworm* (derivado del P-15 *Styx*). Es un gran misil subsónico (≈Mach 0,8) con un alcance de ~80 km, propelente líquido y una ojiva de ~500 kg. Vuela a altitud media-baja (unos cientos de metros) y desciende al detectar el blanco. El 25 de febrero de 1991, las baterías iraquíes lanzaron **dos Silkworm** desde la costa kuwaití ocupada, dirigidos contra las fuerzas navales que apoyaban la ofensiva anfibia de distracción de la coalición.

- **Perfil de detección del buque:** A diferencia de casos anteriores, aquí las defensas estaban alertas y coordinadas. El *HMS Gloucester* asumía la cobertura antimisil de área con sus radares y misiles Sea Dart (sistema de defensa aérea de medio alcance). El *Missouri* contaba con sus propios radares y CIWS Phalanx de defensa cercana. Cuando el Silkworm fue detectado, el *Gloucester* estaba mejor posicionado para reaccionar contra el misil. Los radares Tipo 1022/992Q del *Gloucester* avistaron el misil en acercamiento bastante temprano, según registros británicos, **lo detectaron a unas 21 millas náuticas (~39 km)** de distancia. El eco fue identificado como *misil* antibuque por su perfil de vuelo y trayectoria (vuelo bajo y sin responder a interpelaciones IFF). Dado que el misil entraba rápido en el alcance, el *Gloucester* tuvo segundos para reaccionar, se estimó menos de **1 minuto desde detección hasta impacto potencial**, dada la velocidad del misil de~0,89 Mach.

- **Distancia de detección del misil:21 mn (39 km)** Esto proporcionó alrededor de 90 segundos totales hasta el posible impacto en el acorazado. La detección temprana permitió una respuesta coordinada el *Missouri* lanzó señuelos de chaff inmediatamente para confundir el radar del Silkworm, y *Gloucester* inició un viraje brusco para alinear su lanzador de misiles hacia el blanco.

- **Resultado del ataque: el** *HMS Gloucester* disparó **dos misiles antiaéreos Sea Dart** casi al límite de su envolvente, logrando que uno de ellos interceptara y destruyera el Silkworm en vuelo. La intercepción se logró a unos pocos kilómetros de distancia: diversas fuentes sitúan el punto de derribo a **entre 2,75 y 4 mn (~5–7 km) del *Gloucester***, y **entre 4 y 7 mn (~7–13 km) del *Missouri***. La altitud del encuentro fue de unos pocos cientos de metros (testigos difieren entre 120 m y 300 m de altura). El misil iraquí fue destruido aproximadamente **30 segundos antes** de que hubiera alcanzado al *Missouri*, evitando por completo el daño a las naves de la coalición. Cabe señalar que en la confusión, la fragata USS *Jarrett* activó erróneamente su CIWS Phalanx, que disparó hacia las nubes de chaff de *Missouri* y alcanzó con algunos proyectiles al propio *Missouri*. Un segundo Silkworm lanzado simultáneamente cayó al mar, posiblemente desviado por las contramedidas y sin llegar a ser una amenaza directa.

- **Comentarios:** Este episodio fue el **primer derribo confirmado de un misil antibuque por otro misil lanzado desde buque** en combate. Demostró que, con **detección temprana** y reglas de empeñamiento claras, es posible neutralizar misiles antibuque antes del impacto. La distancia de detección (21 mn) fue favorecida porque el Silkworm volaba más alto que misiles modernos (no era un sea-skimmer puro) y porque *Gloucester* estaba en alerta máxima. Las fuentes varían ligeramente sobre detalles (distancia exacta de intercepción, si hubo un tercer misil que falló por completo, etc.), pero coinciden en el éxito defensivo. La Royal Navy aprovechó el hecho para resaltar la eficacia de sus sistemas, aunque se reconoció la suerte de que el ataque no fuera con múltiples misiles simultáneos o perfiles más bajos. El *Missouri* y sus escoltas mostraron cómo una defensa en capas –chaff, maniobra y misiles antiaéreos– puede enfrentar amenazas de misiles, en contraste con casos previos donde la sorpresa táctica dominó.

2006 – Ataque al *INS Hanit* (Segunda Guerra del Líbano, 2006)

- **Conflicto y buque:** Guerra del Líbano 2006 (Israel vs. Hezbollah); *INS Hanit* es una corbeta israelí clase Sa'ar 5 de 1.200 ton, con avanzados sistemas: radar EL/M-2218S, misiles antiaéreos Barak-1 (alcance 10 km), cañón CIWS Phalanx, señuelos y ESM. Patrullaba 16 km frente a la costa de Beirut como buque insignia durante las operaciones navales.

- **Misil utilizado:** Misil antibuque chino *C-802* (versión iraní Noor), lanzado el 14 de julio de 2006 por la guerrilla Hezbollah desde la costa libanesa. El C-802 es subsónico (≈Mach

0,8), con alcance ~120 km y vuelo *sea-skimming* en fase terminal (vuela a ~5–7 m sobre el mar para evadir radar). Porta una ojiva de ~165 kg. Informes posteriores indicaron que Hezbollah pudo haber disparado **dos misiles simultáneamente**, uno C-802 (que sobrevoló *Hanit* y golpeó a un mercante a 60 km), y otro misil más pequeño (posiblemente un C-701 o Yingji-7 de 30 kg de ojiva) que impactó en *Hanit*. La inteligencia israelí inicialmente no sabía de la capacidad misil de Hezbollah, lo que contribuyó a la sorpresa.

- **Perfil de detección del buque:** Pese a ser un buque moderno, *Hanit* **no tenía sus sistemas antimisiles activados en el momento del ataque**. La Marina Israelí, subestimando la amenaza, no había identificado la presencia de misiles costeros en manos de Hezbollah. En consecuencia, a bordo de la *Hanit* ciertos sistemas se encontraban en modo de espera para ahorro de energía. Un oficial de guardia **había desactivado el radar principal de vigilancia y parte del sistema de defensa** alegando que "el barco no estaba bajo amenaza". Esto significó que el *Hanit* navegaba con su **misil Barak y el CIWS en standby**, sin alerta temprana activa. Normalmente, en ejercicios de paz sí mantenían encendido el sistema automático de alerta de misiles, pero en combate real no lo hicieron por la falsa asunción de que Hezbollah no poseía tales armas. Además, el buque estaba concentrado en operaciones terrestres (dar apoyo con su cañón) y no en defensa aérea.

- **Distancia de detección del misil:** *el buque* **no detectó el misil entrante en absoluto antes del impacto**. Al tener su radar de búsqueda aérea principal apagado, la corbeta quedó prácticamente ciega ante un ataque por sorpresa. No hubo alerta en el puente ni tiempo para reaccionar; ninguna traza de misil fue advertida ni se lanzaron contramedidas. El C-802 (o C-701) voló bajo el radar hasta estrellarse contra el buque. Según se supo, **el sistema de alerta automática estaba en modo ahorro de energía y no emitió ninguna advertencia**. El impacto ocurrió sin previo aviso, muchos miembros de la tripulación ni supieron qué los golpeó hasta después.

- **Resultado del ataque:** El misil impactó en la popa del *Hanit*, cerca de la cubierta de vuelo, a nivel de la línea de flotación. La explosión abrió un boquete y provocó un incendio que destruyó la grúa de carga y dañó la planta propulsora, dejando el buque temporalmente sin propulsión. Cuatro tripulantes fallecieron en la explosión/incendio. Aun así, *Hanit* logró mantener flotabilidad y, una vez controlados los daños, se retiró por sus propios medios hasta el puerto de Ashdod para reparaciones. Un segundo misil disparado en la misma salva pasó de largo (posiblemente el C-802), porque *Hanit* ya había sido alcanzado y no lo adquirió, terminando por golpear a un carguero civil a 50 km mar adentro, hundiéndolo.

- **Comentarios:** Este incidente causó sorpresa y polémica en Israel. Se descubrió que **hubo fallos tanto de inteligencia como operativos**. La inteligencia naval había recibido indicios desde 2003 de que Hezbollah podía tener misiles costeros, pero no se transmitió adecuadamente a la tripulación. Operativamente, hubo **negligencia al no activar el radar y defensas en zona de combate**. Oficiales de la marina israelí fueron reprendidos por haber dejado el barco vulnerable por sobre confianza. La principal lección fue obvia, nunca presumir falta de amenaza. los sistemas de defensa antimisil deben estar siempre activos en zona de peligro. Tras el ataque, Israel reorganizó protocolos para que las corbetas mantengan sus escudos antiaéreos activos incluso ante amenazas no confirmadas, y mejoró la coordinación inteligencia-operaciones. *Hanit* sobrevivió, pero el evento demostró que incluso un buque moderno puede ser sorprendido si **sus sensores no están operativos**.

2016 – Interceptaciones del *USS Mason* (Conflicto en Yemen)

- **Conflicto y buque:** Guerra civil de Yemen (2015-presente), enfrentamientos indirectos entre rebeldes Houthies (apoyados por Irán) y coalición liderada por Arabia Saudita. El *USS Mason* (DDG-87) es un destructor estadounidense clase Arleigh Burke, equipado con el avanzado sistema Aegis (radares SPY-1D de búsqueda aérea 3D) y armamento antiaéreo de última generación: misiles Standard SM-2 de largo alcance, misiles ESSM de medio alcance, CIWS Phalanx, señuelos Nulka, etc.

- **Misil utilizado:** Se cree que fueron **misiles C-802 "Noor"** de fabricación iraní (o su derivado), similares al caso de *Hanit*. El 9 de octubre de 2016, fuerzas Houthi lanzaron **dos misiles de crucero antibuque** contra el *USS Mason* desde la costa del Mar Rojo (estrecho Bab el-Mandeb). Cada misil vuela subsónico (~Mach 0,8) y rasante.

- **Perfil de detección del buque: el buque**, tras un ataque previo a un buque mercante emiratí, estaba en máxima alerta. A las 19:00 hora local, sus radares detectaron las amenazas en el aire. De acuerdo con el Pentágono, el destructor **detectó dos misiles en acercamiento en un lapso de 60 minutos** mientras operaba en aguas internacionales. Inmediatamente el buque ejecutó su plan de defensa multicapa: se activaron las soluciones de tiro y se prepararon contramedidas. El *Mason* empleó su moderno radar SPY-1 para rastrear los blancos y los clasificó como misiles antibuque en vuelo.

- **Distancia de detección del misil:** Los detalles exactos son clasificados, pero dada la exitosa defensa, se infiere que la detección ocurrió **apenas los misiles emergieron sobre el horizonte radar (~10–15 km)**. Posiblemente recibió una alerta por el sistema de ESM del radar del misil o lo avistó en su SPY-1 tan pronto asomó de la costa. De hecho, lanzó sus interceptores cuando los misiles aún estaban lo bastante lejos de la fuerza (quizá decenas de segundos de impacto). Según reportes oficiales, el sistema Aegis *"detectó lo que parecían misiles antibuque entrantes"* y la tripulación reaccionó en consecuencia.

- **Resultado del ataque: el destructor** *USS Mason* respondió eficazmente: **lanzó dos misiles Standard SM-2 y un misil ESSM** contra los dos blancos, además de activar un señuelo electrónico *Nulka*. Esta fue la primera vez que un buque de guerra de EE.UU. disparó misiles antiaéreos en combate real en décadas. Según fuentes del Departamento de Defensa, es incierto si sus misiles derribaron el primer misil o si este cayó al agua por las contramedidas, pero **ninguno de los misiles Houthi alcanzó al Mason ni al buque aliado cercano (USS Ponce)**. El primer misil se neutralizó (por impacto directo o desviación) antes de llegar al grupo naval, y el segundo cayó al mar sin lograr impacto, posiblemente confundido por los señuelos o por fallo de guía. Días después, el *Mason* sufrió un tercer ataque similar (12 de octubre) que igualmente resultó infructuoso. No hubo daños ni bajas en los buques estadounidenses.

- **Controversias o lecciones:** La acción del Uss *Mason* demostró la eficacia de la defensa moderna cuando el buque está preparado. **A diferencia de todos los casos anteriores, aquí la detección fue temprana y la respuesta automática**, derribando o desviando los misiles antes de su fase terminal. Esto confirmó la utilidad del entrenamiento post-*Stark* y los sistemas integrados. Técnicamente, marcó la primera intervención exitosa de misiles SM-2/ESSM en una situación real antimisil. Hubo cierta confusión inicial en informes (el Pentágono inicialmente fue cauto en admitir el lanzamiento de interceptores), pero luego se confirmó que el destructor había empleado armamento defensivo. Este incidente reforzó que incluso misiles obsoletos como el C-802 siguen siendo peligrosos, pero que con alerta adecuada pueden ser contrarrestados. También subrayó la creciente amenaza de actores no estatales con armamento sofisticado, cambiando las reglas de enfrentamiento en zonas costeras conflictivas.

2022 – Hundimiento del crucero *Moskva* (Guerra ruso-ucraniana)

- **Conflicto y buque:** Invasión rusa de Ucrania (2022); el *Moskva* era un crucero lanzamisiles ruso (clase Slava, desplazamiento 12.000 ton), buque insignia de la Flota del Mar Negro. Estaba armado con sistemas antiaéreos de largo alcance (, SA-N-6 versión naval del *S-300F Rif*, con un alcance de 75 km), misiles de corto alcance OSA-MA (SA-N-4) y 6 cañones CIWS AK-630 de 30 mm, además de señuelos. Teóricamente tenía una defensa antiaérea por capas robusta.

- **Misil utilizado:** Misil de crucero antibuque ucraniano *R-360 Neptune*, desarrollado recientemente (2021) a partir del diseño soviético Kh-35. Es subsónico (≈900 km/h), con alcance máximo 280 km, y realiza un perfil de ataque *sea-skimming* (vuelo a 3–5 m sobre el mar en terminal). Lleva una ojiva de 150 kg. El 13 de abril de 2022, las fuerzas ucranianas dispararon **dos misiles *Neptune*** desde la costa cerca de Odessa contra el *Moskva*. Se alega

que usaron un dron TB2 Bayraktar para distraer o localizar al buque. El ataque ocurrió al anochecer, con el *Moskva* a unas 50 mn (≈90 km) de la costa.

- **Perfil de detección del buque:** En teoría, el crucero ruso estaba equipado para detectar y derribar misiles como el Neptune con su red de radares (incluyendo el MR-710 "Top Steer" de búsqueda aérea) y misiles SAM de área. Se calcula que, dado el perfil del misil Neptune, el crucero podría haber tenido **3–4 minutos de advertencia radar** antes del impacto, si sus sistemas hubieran estado plenamente operativos. Esto sería suficiente para encender sus radares de control, lanzar misiles S-300F y preparar CIWS. **Sin embargo, ninguna de sus defensas se activó.** No hay evidencia de misiles lanzados, chaff desplegado ni cañones disparados. Se sospecha que **o bien los radares del *Moskva* no detectaron los Neptune entrantes, o la tripulación no estaba preparada/entrenada para reaccionar**, de modo que el buque fue sorprendido. Algunas fuentes señalan que sus sensores eran obsoletos (tecnología de los 1980s) y optimizados para detectar aviones, no objetivos tan bajos como un Neptune. También se debatió si el dron Bayraktar pudo distraer su atención (aunque analistas sugieren que el TB2 y los misiles atacarían con sistemas diferentes, y el verdadero problema fue la falta de alerta interna).

- **Distancia de detección del misil: Prácticamente nula en la práctica.** Aunque calculado se estima que el *Moskva* debería haber detectado los misiles a decenas de kilómetros (3–4 minutos de vuelo equivalen quizá a 40–50 km), **no lo hizo o no reaccionó en consecuencia**. Esto implica que los Neptune llegaron sin oposición hasta el buque. Un análisis de Defense News con fuentes turcas indicó que el *Moskva* probablemente **"no detectó los misiles entrantes o no estaba listo para enfrentarlos"**, posiblemente por falta de preparación de la tripulación para emergencias. En resumen, la alerta falló completamente, el buque fue completamente sorprendido por el ataque.

- **Resultado del ataque:** Ambos misiles Neptune lograron impacto. Hacia las 20:42 del 13/abril/2022, reportes ucranianos informaban que el *Moskva* estaba "en llamas y escorado" tras ser alcanzado por **dos misiles**. Las ojivas aparentemente detonaron, provocando incendios que alcanzaron depósitos de munición a bordo. El crucero quedó sin control de daños efectivo. Según la versión rusa, una explosión de municiones por un "incendio accidental" causó daños catastróficos. Los rusos reconocieron la necesidad de evacuar la tripulación. Durante la noche, mientras era remolcado con mal tiempo, el buque se hundió el 14 de abril. Se desconoce el número de bajas (Rusia afirmó rescatar a la mayoría, pero fuentes extraoficiales sugieren decenas de muertos). El buque se perdió por completo, marcando la mayor nave de guerra hundida en combate desde 1945.

- **Comentarios:** El hundimiento del crucero *Moskva* confirmó la letalidad de los misiles costeros modernos y evidenció **fallos graves en la doctrina y estado técnico ruso**. Hubo debate si EE.UU. asistió con inteligencia (identificando la posición del *buque*), pero en cualquier caso la ejecución fue ucraniana. La principal controversia interna fue cómo un crucero con supuesta defensa multicapa fue tomado por sorpresa. La falta de reacción sugiere o **confianza excesiva**, **posible malfuncionamiento** de radares (dadas sus décadas de servicio sin gran modernización) o **entrenamiento deficiente** para escenarios de saturación. **Este incidente, unido al de *Hanit* 2006, muestra que tener sistemas avanzados no garantiza protección si no están operados adecuadamente en el momento preciso**. Tras la pérdida, analistas destacaron que la guerra moderna revaloriza los misiles antibuque y que buques mayores deben complementarse con buenas tácticas (dispersión, alerta continua, escoltas) para no ser blancos fáciles. Para Ucrania, el caso elevó la reputación de sus misiles Neptune e incentivó a otros países a robustecer sus defensas costeras.

Conclusiones

A lo largo de estos casos históricos –desde las primitivas bombas guiadas de la SGM hasta los misiles inteligentes actuales– se observa una evolución tanto de la amenaza como de la defensa:

- **Errores humanos y de apreciación:** Casi todos los casos donde el buque fue alcanzado comparten algún elemento de **error humano**, como subestimar la amenaza (*Sheffield*, *Hanit*, *Moskva*), malinterpretar la señal (*Khaibar* pensando en aviones), falta de

entrenamiento o reglas de enfrentamiento estrictas (*Stark*). Por otro lado, cuando las dotaciones actuaron correctamente(*Gloucester*, *Mason*), se pudieron evitar impactos. La **cultura de estar siempre en guardia** frente a misiles antibuque parece escrita con sangre en la historia naval.En resumen, la historia de los ataques con misiles antibuque muestra un aprendizaje costoso. Los valores de distancia de detección han mejorado con la tecnología (de meros alcances visuales a decenas de km por radar moderno), pero la física impone límites como en el vuelo rasante. Cada conflicto ha aportado lecciones que han refinado las defensas: de no tener aviso en 1943, a interceptar misiles en vuelo en 1991 y 2016. Aún así, los casos recientes advierten que la **complacencia** o las **deficiencias en preparación** pueden volver inútiles incluso a los sistemas más avanzados, con consecuencias fatales.

- **Horizonte radar y vuelo rasante:** Gran parte de los éxitos de misiles antibuque se explican por volar a baja altura, explotando la curvatura terrestre para **ocultarse del radar hasta último momento**. En 1982, *Sheffield* no vio el Éxocet; en 1987, *Stark* solo lo vio al final; en 2006, *Hanit* ni lo buscó; en 2022, *Moskva* aparentemente tampoco lo detectó a tiempo. Hoy se entiende que el horizonte radar para un blanco a pocos metros del agua es de apenas18–20 km (dependiendo de la altura del mástil), dando segundos de reacción. Los buques modernos han incorporado radares de múltiples bandas y **alertas automatizadas** para atenuar este problema, pero sigue siendo un factor crítico.

- **Tiempo de reacción y automatización:** En casos de detección tardía, el tiempo disponible se mide en segundos. Por ejemplo, un Éxocet a 0,93 Mach cubre 500 m por segundo; detectar a 10 km da 20 s de respuesta. Solo sistemas automáticos o tripulaciones en alerta máxima pueden reaccionar tan rápido. Esto destaca la necesidad de **integrar sensores y armas** (como Aegis) que automaticen la secuencia detectar-atacar. Cuando esto ocurrió, como en los casos del *Gloucester* 1991 o el *Mason* 2016, los misiles enemigos fueron neutralizados a tiempo. De lo contrario, los impactos fueron casi inevitables.

- **Contramedidas electrónicas y señuelos:** Varios incidentes revelan la importancia de la guerra electrónica. En 1943 los Aliados aprendieron a **inhibir las señales** del Fritz X. En 1967 y 1971, los buques carecían de ECM, sufriendo impactos directos. En 1982-87 se empleó chaff con cierto éxito limitado (p.ej., *Yarmouth* lanzó chaff aunque el Éxocet igualmente alcanzó a *Sheffield*). En 1991, *Missouri* y *Gloucester* usaron chaff para desviar al misil Silkworm. En 2016, *Mason* usó señuelos *Nulka* que pudieron hacer errar a un misil . Esto muestra que las contramedidas pueden reducir la probabilidad de impacto, pero deben ser desplegadas a tiempo, lo que regresa al punto de la detección oportuna.

Jhon C Schulte

En su trabajo "Análisis histórico de la efectividad de los misiles de crucero antibuque en la guerra del litoral", de 1988, Jhon C Schulte clasifico los casos históricos en tres categorías. Blancos indefensos como los buques mercantes, buques de guerra que no se defendieron y buques de guerra que se defendieron. Esto nos permite a modo de resumen histórico, justipreciar las posibilidades de defensa real de un buque bajo el ataque de misiles de crucero.

	Probabilidad de de impactos totales	Probabilidad después de 1982 hasta 1988
Blancos indefensos	91.3 %	98,1 %
Buques de guerra que no se defendieron	68,4 %	63 %
Buques de guerra que se defendieron.	26,4 %	45 %

Conclusiones

Los misiles son armas letales si se les permite desarrollar su potencial según su diseño, como se manifiesto contra buques mercante . Los buques de guerra, debido a su preparación para el

combate de su dotación. compartimentación y capacidades de control de averías logran reducir la probabilidad de impacto, pero aquellos que reaccionaron y se defendieron muestran que lla defensa se puede imponer al ataque.

Doble Tap

Los misiles antiaéreos se lanzan comúnmente en parejas, la causa de esto es múltiple pero la principal es estadística y se pone de manifiesto en la siguiente tabla.

Probabilidades combinadas de impacto

Pk individual	Probabilidad con 1 misil	Probabilidad con 2 misiles	Probabilidad con 3 misiles
60%	0.6	0.84	0.936
70%	0.7	0.91	0.973
80%	0.8	0.96	0.992
90%	0.9	0.99	0.999

Al lanzar dos misiles, la probabilidad combinada de destruir el objetivo se incrementa considerablemente. Según la siguiente formula

$$P(\text{al menos uno acierta}) = 1 - (1 - Pk)^2$$

también se verifica que cuanto menor es la probabilidad de impacto con un misil mas significativa es el resultado de la suma. Al incrementarse la probabilidad de impacto con un misil hay que empezar a considerar si es conveniente el doble lanzamiento ya que se consume el doble de munición para una mejora en la probabilidad de impacto marginal. También se pone de manifiesto que el lanzamiento de tres misiles no es conveniente debido al alto consumo de municiones con una mejora poco significativa de la probabilidad de impacto total.

A la causa puramente estadística se suma el reducido tiempo que se tene para empeñarse contra el blanco por lo que no resulta conveniente lanzar, esperar el resultado y relanzar si no se consigue un impacto. Es también conveniente para sobreponerse a las fallas técnicas en la guía, propulsión o problemas del misil.

» La Ingeniería Social y sus Implicancias

Por TN Lic. Maximiliano Daniel Gamboa [3]

El presente pertenece a un estudio más amplio titulado "Concienciación en Ciberseguridad para la preservación del poder de combate".

Introducción

Este artículo tiene como objetivo ser el primero de una serie dedicada a comprender las amenazas en el ciberespacio, y la importancia del adiestramiento y la comprensión de los riesgos transversales a los que estamos expuestos el personal militar. Además, buscará que los lectores tomen conciencia del impacto que el comportamiento en el ciberespacio puede tener en la preservación del poder de combate.

En primer lugar, debemos conceptualizar el Ciberespacio, entendiendo al mismo como el *"dominio global y dinámico compuesto por las infraestructuras de tecnología de la información, incluida Internet, las redes y los sistemas de información y de telecomunicaciones, tiene entre otras, como características esenciales, su dimensión global y transfronteriza, su naturaleza dual, su masividad y su vertiginosa y constante evolución."*[4] No obstante lo mencionado, hay un factor muy importante a tener en cuenta cuando hablamos del ciberespacio, y es el factor humano como componente esencial para el funcionamiento del mismo, ya que las personas crean, modifican, realizan actividades, funciones y operaciones en él.

Por ello, se debe buscar el fortalecimiento del personal que integra nuestra fuerza, como primera barrera frente a un ciberataque, además de la protección de las infraestructuras de la información. Los atacantes tienen este hecho muy claro, por esta razón buscan explotar las debilidades del factor humano al atacar una organización, y los militares no somos la excepción.

---

[3] Teniente de Navío, licenciado en Recursos Navales para la Defensa. Orientación Comando Infantería de Marina

[4] Estrategia Nacional de Ciberseguridad de la República Argentina, 2019. Recuperado de https://www.argentina.gob.ar/sites/default/files/infoleg/res829-01.pdf

En el ámbito naval, donde el aislamiento prolongado, la fatiga operacional y la dependencia en sistemas informáticos críticos son constantes, estas vulnerabilidades humanas se vuelven particularmente peligrosas. En este contexto, la ingeniería social se ha posicionado como una amenaza estratégica capaz de afectar significativamente la capacidad operacional de fuerzas militares, tal y como lo veremos a continuación.

¿Qué es la ingeniería social?

Cuando un adversario desea obtener información de relevancia de una organización, comienza su accionar con técnicas de reconocimiento. Una de estas técnicas es la ingeniería social.

La ingeniería social, es definida por la Asociación de la Industria de Tecnología de la Computación (Computing Technology Industry Association – CompTIA) como el conjunto de métodos empleados por hackers[5] para ganarse la confianza de un usuario final y así obtener información que les permita acceder a datos o sistemas, persuadiendo o influyendo en la persona para que esta brinde cierta información de forma voluntaria o involuntaria. La ingeniería social como herramienta, no produce efectos por si misma, pero provee de los recursos necesarios para ingresar a una red e impactar en ella, por lo tanto, a menudo es precursora de otros tipos de ataques.

Antes de realizar un ataque de ingeniería social, los adversarios tratan de obtener información sobre la organización objetivo de diversas fuentes, como la página oficial u otras redes donde ellos revelan identificación de su personal, nombres y dirección de correos; blog, foros en los cuales los subordinados revelan información personal e información organizacional. A esto se lo llama "reconocimiento".

Luego del reconocimiento, y de haber obtenido la información suficiente sobre la organización objetivo, se busca obtener acceso y persistencia en el sistema enemigo, mediante la ingeniería social, mediante técnicas como la suplantación, el acceso, la persistencia y la ingeniería social inversa.

Un ejemplo de una acción de Ingeniería Social es el siguiente:

Durante la Copa Mundial de la FIFA 2018, Hamás creó una aplicación para explotar el interés de los aficionados en los partidos. Supuestamente, permitía a los usuarios seguir los resultados, pero también contenía malware[6] dirigido al personal de las Fuerzas de Defensa de Israel (FDI). Esto permitió a Hamás controlar las cámaras y los micrófonos de los teléfonos a distancia, obteniendo información sobre las tropas, bases, equipos y operaciones de las FDI. Los hackers asociados a Hamás han demostrado su habilidad para usar la ingeniería social en aplicaciones de mensajería populares como WhatsApp para obtener información. Los dispositivos de las FDI pirateados parecen haber proporcionado gran parte de la información sorprendentemente detallada sobre plataformas e instalaciones de armas que contribuyó al éxito de los ataques del 7 de octubre. (Major W. Stone Holden, 2024)

En el ejemplo anterior, se puede con claridad el público objetivo de la campaña de ingeniería social y el impacto posterior, tras la explotación de la información obtenida.

Phishing y ataques relacionados

El "phishing" es un tipo de ataque común de ingeniería social basado en correo electrónico, como, por ejemplo, lo siguiente:

"Ha salido a la luz una reciente campaña de espionaje cibernético dirigida a la Armada de Pakistán, que pone de manifiesto la creciente sofisticación de los actores de amenazas que operan en la región del sur de Asia. [...] El ataque comenzó con un documento PDF malicioso que se hizo pasar por un memorándum interno de T[7]I para la comunicación segura por correo electrónico. Las víctimas fueron engañadas para que instalaran una extensión de Thunderbird[8] mezclada con

[5] Un hacker es una persona con habilidades técnicas avanzadas capaz de entender y modificar un sistema informático.
[6] "Malware" es la palabra con la que se conoce al Software malicioso. Su nombre proviene de la combinación de las palabras "Malicious" y "Software".
[7] Haciendo referencia al sector de Sistemas o Tecnologías de la Información.
[8] "Thundebird" es una aplicación de correo electrónico de la fundación Mozilla.

malware a través de una URL con errores tipográficos que se asemejaba a dominios legítimos de la Armada de Pakistán. […] El malware recopiló tipos de archivos específicos y los preparó para su exfiltración mediante cifrado dinámico" (Dryad Global, 2024)

Generalmente, un ataque de phishing afirmará que una acción de la víctima es necesaria por motivos de seguridad, como una validación de cuenta, ingresar a un link y cambiar un dato, descargar un archivo, etcétera. Por ello nunca se debe proporcionar información personal o de la Institución, sea por correo electrónico o por teléfono, ni dar click en enlaces no verificados[9].

La ingeniería social es el principal vector de ataque inicial, y de él deriva "Spear Phishing[10]". Este ataque va dirigido a un individuo o una institución específica, como podría ser la figura de un Comandante o Director, o la Armada Argentina. El "Spear phishing" utiliza correo electrónico al igual que el phishing para llegar a las víctimas. Por ejemplo:

> 1) *Un grupo de piratas informáticos vinculado a la inteligencia rusa intentó infiltrarse en los sistemas de docenas de centros de investigación, periodistas y ex funcionarios militares y de inteligencia occidentales.*

El grupo, conocido como Star Blizzard (…), dirigía a sus víctimas correos electrónicos que parecían provenir de una fuente confiable, una táctica conocida como "Spear Phishing". De hecho, los correos buscaban acceder a los sistemas internos de las víctimas para robar información e interrumpir sus actividades. […] Las autoridades no han entrado en detalles sobre la eficacia de Star Blizzard, pero dijeron que esperan que Rusia siga realizando hackeos y ciberataques contra Estados Unidos y sus aliados. (Klepper, 2024).

Otras variantes relacionadas con el phishing, que se pueden presentar, son:

- Pharming: Representa la suplantación de un sitio web legítimo que tiene como propósito engañar a los usuarios para que ingresen sus credenciales y robar información.
- Vishing: Es una práctica de suplantación de identidad mediante el uso de la tecnología de comunicación de voz.
- Smishing: Es un técnica de suplantación de identidad mediante la mensajería de texto en los teléfonos móviles.

Spam.

Los correos "spam", o "correo basura", son correos electrónicos no solicitados. Estos pueden ser utilizados para enviar enlaces dañinos, malware o contenido engañoso, destinados a robar información.

Algunos de los indicadores más comunes de correo no deseado son los siguientes.

- El correo electrónico no tiene asunto.
- Normalmente solicita la actualización de una cuenta.
- El texto tiene palabras mal escrita o puntuación extraña.
- Los enlaces son largos, se parece a una correspondencia de una empresa legítima.
- Finalmente, dicho correo solicita que el usuario abra un archivo adjunto.

Difícilmente una persona de la institución reciba correo SPAM a su casilla de correo institucional, salvo que se haya vinculado el correo a algún sitio web sospechoso, o se haya suscrito a algún sitio y el mismo haya sido víctima de una brecha de datos. De todas formas, si se recibe un correo electrónico que contiene uno o más de los indicadores mencionados, es conveniente no abrirlo o marcarlo como SPAM.

Hoaxes o engaños

[9] Los enlaces pueden ser verificados en herramientas como "Virus Total", en https://www.virustotal.com/gui/home/url
[10] Spear phishing: Ataque de phishing dirigido.

Los "hoaxes", también conocidos como engaños, son una forma de ataque que se difunde a través de correos electrónicos, mensajes instantáneos o sitios web, con la intención de manipular al usuario para que tome decisiones inapropiadas, como eliminar archivos importantes del sistema.

Estos ataques, que forman parte de las estrategias de ingeniería social, suelen tener mayor efecto sobre personas con poca experiencia en el manejo de tecnología. Para lograr su propósito, el mensaje suele captar la atención del usuario, presentar una amenaza creíble y, finalmente, inducir una acción. Un ejemplo típico sería un aviso que informa sobre supuestos cambios en los términos de uso de una aplicación, generando una sensación de urgencia para instalar una extensión que, en realidad, es un software malicioso.

Técnica de "Impersonation" o suplantación de identidad

"Impersonation" o suplantación de identidad es un ataque humano en el cual un adversario pretende ser quien no es, persiguiendo objetivos de los más variados (extorsión, manipulación, robo de información, etc). Un ejemplo de esto es el siguiente:

Caso OTAN – Suplantación en redes sociales (2012) Agentes chinos crearon perfiles falsos en Facebook, haciéndose pasar por el almirante James Stavridis, entonces comandante supremo de la OTAN. Mediante estas cuentas falsas lograron obtener información militar sensible al aprovechar relaciones personales de confianza, evidenciando la vulnerabilidad del alto mando frente a ataques sofisticados de ingeniería social. (The Guardian, 2012)

Si la identidad no puede ser verificada fácilmente, las probabilidades de que este tipo de ataques sean exitosos, son altas. Si el personal militar no reconoce a la autoridad con quien se está comunicando, o no tiene preestablecido el canal de comunicación con su superior, eso ya es razón suficiente para sospechar. La suplantación de identidad puede darse tanto en redes sociales, como en servicios de mensajería como "Whatsapp", y usar la identidad de un militar para solicitar dinero o favores.

Generalmente ataque de suplantación exitoso depende de cuan detallada sea la investigación de la víctima, y sus antecedentes, de cuanta confianza pueda construir un atacante con su víctima, y de la habilidad y creatividad del atacante para desplegar sus armas con la información recabada.

Para evitar estos tipos de ataques, desde la Institución se deben tomar iniciativas para proporcionar capacitación proactiva de concienciación sobre ciberseguridad al personal militar, que permitan que estos aprendan sobre las metodologías del ataque cibernético y las diferentes formas en que estos hechos puedan aplicarse a ellos y perjudicar a la Armada Argentina.

Una variante de "impersonation", y elegido por los atacantes, es el "catfishing", que consiste en la creación de perfiles falsos para explotar la debilidad del personal militar por el sexo opuesto, como en el ejemplo a continuación:

Utilizando avatares femeninos de Skype, los atacantes se hicieron pasar por "mujeres aparentemente simpáticas y atractivas" que, en algún momento de la conversación, atrajeron a las víctimas para que abrieran fotos personales que en realidad eran malware.

El informe señaló que los atacantes solían preguntar a las víctimas si estaban usando su computadora o dispositivo móvil para enviarles el malware correspondiente. […] Otras herramientas maliciosas en el arsenal del grupo de amenazas eran el troyano de acceso remoto (RAT) DarkComet y un keylogger[11] personalizado. Los datos militares obtenidos por los atacantes incluían información sobre material militar y las posiciones de los grupos combatientes, los nombres de los combatientes y sus sistemas de armas, listas de beneficiarios de ayuda a refugiados y bajas, registros de esfuerzos y financiación humanitaria, y comunicaciones sobre estrategia política y planificación militar. (Walker, 2015)

Técnicas "typosquatting"

[11] Keylogger: Se trata de un software que captura las señales del teclado, registrando todo lo que escribe una persona.

El "typosquatting[12]" es una técnica en la que se explota las fallas ortográficas al momento de escribir direcciones web en la barra de nuestro navegador, y suele ser empleado junto a la técnica de phishing.

Para explotar el "typosquatting", los atacantes buscan cambiar, sustituir u omitir algunas letras de los URL para hacer que un dominio fraudulento se confunda con el original, de modo de aprovechar la confianza que inspira el sitio original para alcanzar objetivos fraudulentos.

En el caso de las técnicas de "typosquatting", consiguen que las direcciones web y los dominios de las direcciones de correo sean prácticamente idénticas a las originales. Para ello, se valen de la homografía, que es el hecho de que caracteres tengan un aspecto similar.

Ejemplo de typosquatting utilizando homografía.

El consejo para evitar caer en este tipo de actos es emplear las páginas guardadas en el navegador, en lugar de ingresar a las mismas a través del buscador.

Ataque de "watering hole"

El ataque de "watering hole[13]" es un método en el que el atacante busca comprometer a un grupo específico de usuarios finales al infectar sitios web que los miembros de ese grupo visitan.

Lo que hace que estos ataques sean difíciles de detectar es que tienden a centrarse en sitios web legítimos y populares. Los atacantes estudian los sitios web de confianza de la organización objetivo (de los cuales recaban información) y los "envenenan" o infectan con malware. Esto permitirá a los atacantes tomar el control del equipo del empleado y poder así espiar y robar información de la compañía.

Estos ataques de se vuelven más efectivos cuando se combinan con mensajes de correo electrónico para atraer a los usuarios a sitios web.

Campañas de influencia

[12] Proviene de la unión de *typo* (que se traduce como error ortográfico) y *squatting* (que se traduce como ocupar, en este caso un dominio web)
[13] O también conocido como "ataque de abrevadero".

Un aspecto en que se destacan, y enmarcan, las campañas de ingeniería social, son las Campañas de influencia. Estas consisten en la recopilación de información táctica sobre un adversario con el fin de utilizarla en su contra, lo que facilita la implementación de tácticas destinadas a influir en sus procesos de tomas de decisiones, por medio de acciones como la difusión de propaganda en pos de adquirir una ventaja competitiva.

Estas campañas suelen estar orientadas a debilitar la confianza colectiva en las instituciones, aprovechando una serie de debilidades predecibles dentro de la organización enemiga.

En este contexto, la ingeniería social sirve como herramienta para el reconocimiento interno de una organización, sus autoridades, procesos, debilidades, factor psicosocial, cultura, comunidad, etc. La combinación de estos elementos aumenta la probabilidad de éxito en una campaña de influencia.

La rapidez en la detección y respuesta de estas acciones es crucial, dado que esto impide que el enemigo tome precauciones para detener o que la campaña sea neutralizada. La reacción o prevención, conlleva el trabajo mancomunado de la organización militar, con la comunidad de inteligencia.

Vale mencionar, que este tipo de acciones no son conducidas por el instrumento militar, sin embargo, deben ser reconocidas como una forma de acción hostil que persigue objetivos específicos a través de la manipulación de la información.

Conclusión

A lo largo del artículo hemos visto ejemplos de personal militar, o de la comunidad de defensa, siendo víctimas de la Ingeniería Social. Todos tienen en común la exfiltración de información como propósito, apuntando contra blancos de alto valor, sea por su acceso, o por el ámbito en que se desenvuelven, para obtener información de valor estratégico.

Debe tenerse en cuenta que este tipo de hechos, pueden afectar de muchas formas a la Institución:

- Robo de información: Las acciones de ingeniería social permiten a la inteligencia enemiga desarrollar apreciaciones más concretas y planificar operaciones más eficaces, y se corre el riesgo significativo de perder gran potencial de combate propio por medio de acciones de sabotaje.
- Moral: La ingeniería social, cuando se detecta, tiene el potencial para afectar a la moral de la propia tropa, quien es víctima de estas técnicas. Además, puede generar daños a largo plazo en la reputación institucional y la confianza interna dentro de las fuerzas.
- Contrainteligencia: De la mano de las consecuencias económicas que pueden afectar a un militar, al ser víctima de una estafa por medio de la ingeniería social, se encuentra asociado el riesgo que representa el personal con problemas económicos. Esto se justifica en el hecho que, para la inteligencia enemiga, el personal con problemas económicos es un recurso fácilmente explotable para obtener información clasificada a cambio de dinero.

Es importante destacar que, tal y como dice Bryan Skarda en su trabajo "Operacionalizando la Ingeniería Social", esta es una herramienta que tiene impacto directo tanto en adversarios como en tropas propias, destacando como influye en los ciclos de toma de decisión, al generar confianza en los propios, e inseguridad en los enemigos (Bryan Skarda, 2008). Esto se debe a que, incluso cuando los ataques de ingeniería social sobre autoridades no sean exitosos, estas metodologías generan la incertidumbre en el enemigo, mermando la confianza en lo confiable de su información.

Es por ello por lo que las fuerzas militares deben implementar estrategias integrales de ciberseguridad que no solo se enfoquen en defensas técnicas, sino que también consideren la concienciación del personal de la Armada. Programas regulares de entrenamiento y sensibilización específicos en técnicas de detección y prevención de ingeniería social, junto con simulaciones realistas de amenazas digitales, son vitales para construir una resistencia efectiva frente a estos ataques.

En definitiva, asegurar el poder naval moderno exige no solo proteger la integridad física de las plataformas, sino también salvaguardar la fortaleza mental y la capacidad crítica del personal

militar frente a las técnicas de manipulación y engaño de la ingeniería social.

Bibliografía

- Bryan Skarda, M. (2008). Operationalizing Social Engineering for Offensive Cyber Operations. Air Force Institute of Technology. Recuperado el 17 de marzo de 2025, de https://scispace.com/pdf/operationalizing-social-engineering-for-offensive-cyber-2l5a0ncivm.pdf
- Cybersecurity, C. C. (2024). Targeted manipulation: Iran's social engineering and spear phishing campaigns. Recuperado el 17 de marzo de 2025, de https://www.cyber.gc.ca/sites/default/files/cyber-iran-social-engineering-spear-phishing-campaigns-e.pdf
- Dryad Global. (21 de noviembre de 2024). Suspected Nation-State Cyber Espionage Targets Pakistan Navy. Dryad Global. Recuperado el 12 de abril de 2025, de https://channel16.dryadglobal.com/suspected-nation-state-cyber-espionage-targets-pakistan-navy?utm_campaign=Ch16%20Notification&utm_source=hs_email&utm_medium=email&_hsenc=p2ANqtz-9CvD-PsYjGSlAtwmZfx3yV2EcGG7E7EcwOfjd26cvYKcCcXR1gT9mfRDPBiIgNJZ2J-VxR
- ESET. (2021). Manual de ingeniería social | Cómo actuar de la manera correcta. Recuperado el 11 de abril de 2025, de https://www.eset.com/fileadmin/ESET/LATAM/pdf/ESET_Social_engineering_handbook_v6_.pdf
- Keepnet Labs. (14 de octubre de 2024). Top 40 phising statics and trend you must know in 2025. Recuperado el abril de 2025, de https://keepnetlabs-com.translate.goog/blog/top-phishing-statistics-and-trends-you-must-know?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge
- Klepper, D. (03 de octube de 2024). The US and Microsoft disrupt a Russian hacking group targeting American officials and nonprofits. Recuperado el 17 de marzo de 2025, de https://apnews.com/article/russia-hacking-microsoft-star-blizzard-fb41bfccbbe7aaecd10a0a93905d4c8a
- Major W. Stone Holden, U. M. (junio de 2024). The Soft Cyber Underbelly of the U.S. Military. U.S. Naval Institute. Recuperado el 17 de marzo de 2025, de https://www.usni.org/magazines/proceedings/2024/june/soft-cyber-underbelly-us-military
- Maundril, B. (9 de diciembre de 2024). Companies, Phishing Scam Targets Ukrainian Defense. Infosecurity Magazine. Recuperado el 17 de marzo de 2025, de https://www.infosecurity-magazine.com/news/phishing-scam-targets-ukrainian/
- Team, C. 4. (05 de julio de 2024). Ciberataques contra el sector de la defensa. Un nuevo frente bélico. Tarlogic - Cybersecurity Experts. Recuperado el 17 de marzo de 2025, de https://www.tarlogic.com/es/blog/ciberataques-contra-el-sector-de-la-defensa/
- The Guardian. (11 de marzo de 2012). China suspected of Facebook attack on NATO's supreme allied Commander. The Guardian. Recuperado el 12 de abril de 2025, de https://www.theguardian.com/world/2012/mar/11/china-spies-facebook-attack-nato
- Vennon, T. (05 de junio de 2007). Social Engineering the Troops. State of Security. Recuperado el 17 de marzo de 2025, de https://stateofsecurity.com/social-engineering-the-troops/
- Walker, D. (2 de febrero de 2015). Hackers used social engineering to glean military intel on Syrian opposition. SC Media. Recuperado el 17 de marzo de 2025, de https://www.scworld.com/news/hackers-used-social-engineering-to-glean-military-intel-on-syrian-opposition
- Zorz, Z. (20 de enero de 2018). British teenager hacked top ranking US officials using social engineering. Help NetSecurity. Recuperado el 17 de marzo de 2025, de https://www.helpnetsecurity.com/2018/01/22/hack-social-engineering/
- CompTIA Security+ Study Guide (6ª ed.). Wiley. SY0-601)

» El rol de la inteligencia de fuentes abiertas en las operaciones navales contemporáneas

Por TN Lic. Bernardo Collado [14]

Aplicaciones tácticas, riesgos emergentes y lecciones observadas en conflictos recientes.

Nitti, M. E., Riedlbauer, D., & Li, L. (2024). Uso de MarineTraffic para seguridad marítima. The Counterterrorism Group.

[14] Teniente de Navío, Oficial de Cuerpo Comando. Licenciado en Recursos Navales para la Defensa y Licenciado en Relaciones Internacionales.

En este contexto, la Inteligencia de Fuentes Abiertas (OSINT) ha emergido como una herramienta fundamental para la obtención, verificación y análisis de información en escenarios navales contemporáneos. Desde imágenes satelitales comerciales hasta datos de tráfico marítimo en tiempo real, pasando por publicaciones en redes sociales y plataformas de monitoreo civil, el OSINT proporciona una ventana valiosa hacia las dinámicas operacionales de buques, puertos, ejercicios navales y amenazas emergentes.

La creciente accesibilidad de fuentes abiertas, sumada a la rápida expansión de sensores distribuidos, redes civiles de observadores y tecnologías geoespaciales comerciales, ha transformado profundamente los modos en que actores estatales y no estatales acceden y procesan información estratégica. Este fenómeno ha alterado el equilibrio de la inteligencia naval: lo que antes requería medios costosos o capacidades clasificadas, hoy puede obtenerse con herramientas de bajo costo y alta precisión.

Este artículo se propone analizar el rol actual del OSINT en el ámbito naval, sus aplicaciones tácticas y operacionales, sus riesgos inherentes y las lecciones observadas en conflictos como el del Mar Rojo y el Mar Negro. Se abordarán fuentes, herramientas, usos doctrinarios y desafíos, destacando el modo en que esta disciplina —hasta hace poco marginal en el campo militar— se ha convertido en una capacidad estratégica de uso dual, accesible tanto a fuerzas regulares como a actores insurgentes, piratas o grupos híbridos.

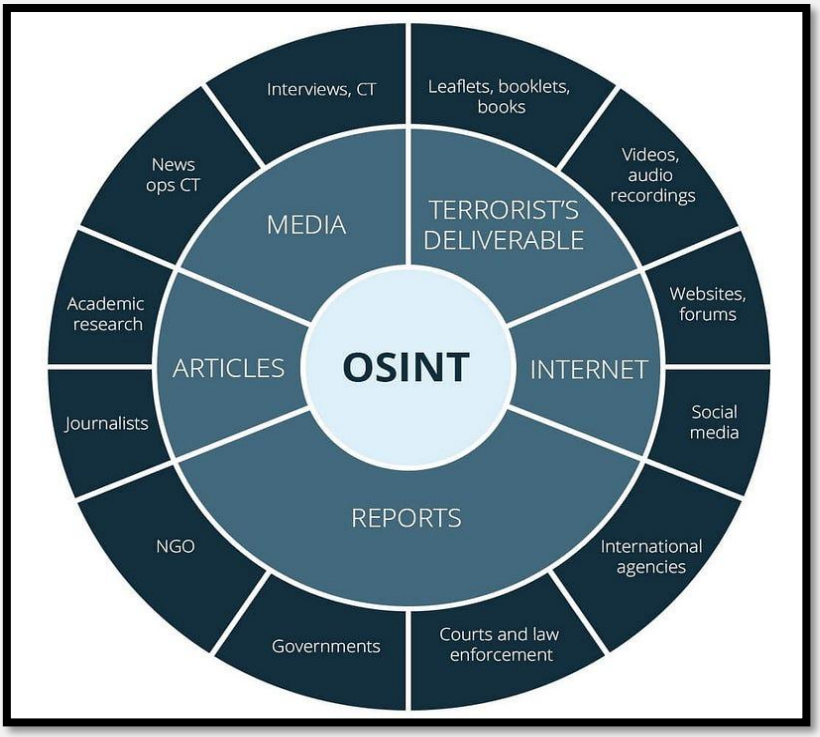
LA INTELIGENCIA DE FUENTES ABIERTAS (OSINT): DEFINICIÓN Y EVOLUCIÓN.

La inteligencia de fuentes abiertas, conocida como OSINT (*Open Source Intelligence*), refiere al proceso de recopilación, análisis y explotación de información disponible al público, que puede ser obtenida legalmente sin recurrir a fuentes clasificadas. Según la Defense Intelligence Agency (2024), el OSINT es "información derivada de fuentes disponibles al público, que incluye medios de comunicación, datos académicos, observaciones técnicas, redes sociales, entre otras, procesadas con fines de inteligencia".

A diferencia de otras disciplinas como la inteligencia humana (HUMINT) o de señales (SIGINT), el OSINT se nutre del entorno digital y globalizado, que ha democratizado el acceso a datos antes reservados a gobiernos o grandes corporaciones. La masificación de satélites comerciales, sensores en tiempo real y redes distribuidas de usuarios ha generado una proliferación de fuentes que, bien analizadas, pueden ofrecer información crítica sobre movimientos militares, patrones logísticos, infraestructura portuaria o despliegues navales.

Su evolución ha sido meteórica. Hasta principios del siglo XXI, el OSINT era considerado un insumo de bajo valor añadido.

Sin embargo, eventos como la Primavera Árabe, la guerra en Siria y, más recientemente, el conflicto entre Rusia y Ucrania, consolidaron al OSINT como una herramienta clave para entender dinámicas operativas en tiempo casi real. Hoy, organismos como la NATO OSINT Centre of Excellence o el United States Naval War College estudian su valor estratégico y su integración en los ciclos de inteligencia multidominio.



Knowlesys. (s.f.). Imagen sobre el marco OSINT. Knowlesys OSINT Academy.

Cabe señalar que el OSINT, a pesar de su acceso público, no es trivial ni inmediato. Requiere metodologías específicas, entrenamiento analítico riguroso y capacidades de verificación cruzada. El desafío no reside en la falta de datos, sino en la sobreabundancia: filtrar, contextualizar y sintetizar información fiable se vuelve una competencia esencial en el siglo XXI, tanto para analistas de escritorio como para operadores en el teatro de operaciones.

El OSINT en el ámbito militar.

El uso de inteligencia de fuentes abiertas en el ámbito militar ha dejado de ser una práctica marginal o auxiliar para convertirse en un componente estructural del ciclo de inteligencia.

En particular, su aplicación se ha visto reforzada por las operaciones multidominio, donde la rapidez en la toma de decisiones exige integrar datos provenientes de fuentes clasificadas y abiertas en tiempo casi real. La posibilidad de **recolectar información desde redes sociales, plataformas comerciales de geointeligencia y transmisiones abiertas** permite obtener indicios tempranos de actividad enemiga, preparar el terreno para operaciones cinéticas o advertir cambios en los patrones logísticos y tácticos de un adversario.

En doctrinas recientes —como el *Multi-Domain Operations Concept* del Ejército de los EE. UU. o las adaptaciones OTAN sobre inteligencia interagencia— el OSINT figura como una fuente prioritaria en fases de planeamiento y alerta temprana. La experiencia en Ucrania es ilustrativa: desde enero de 2022, analistas civiles y militares pudieron detectar acumulaciones rusas en las fronteras, movimientos de blindados y material logístico a partir de imágenes comerciales y reportes geolocalizados por civiles. No fue la inteligencia técnica de alto nivel lo que dominó la narrativa, sino el acceso abierto y descentralizado al conocimiento del terreno (Sutton, 2023).

En el ámbito marítimo, esto se traduce en una capacidad táctica concreta: detectar anticipadamente patrones de navegación sospechosos, identificar embarcaciones camufladas, descubrir centros de reabastecimiento flotantes o vigilar actividades portuarias adversarias. Herramientas como **MarineTraffic**, **VesselFinder** y **SkyWatch** permiten rastrear embarcaciones con señales AIS

(Automatic Identification System) activas, pero también analizar tendencias históricas, rutas evasivas o apagones tácticos. Estas herramientas son empleadas tanto por analistas navales como por actores insurgentes, lo que exige una contramedida adecuada de negación y disuasión.

No obstante, la creciente sofisticación del OSINT militar también ha expuesto su talón de Aquiles: la **veracidad y validación de las fuentes**. La proliferación de desinformación, imágenes manipuladas, reportes sin corroborar y estrategias de *deception* obliga a integrar al OSINT dentro de una matriz analítica rigurosa, apoyada por inteligencia técnica, señales y humana.

Aun así, su valor táctico es innegable: **facilita decisiones rápidas, baja el umbral tecnológico de entrada y extiende la capacidad de observación más allá de las fronteras tradicionales del conflicto.**

El OSINT en operaciones navales contemporáneas.

En el entorno marítimo, donde el dominio del espacio, el tiempo y la distancia ha sido históricamente una ventaja de las grandes armadas, la aparición del OSINT ha introducido una **variable disruptiva**. Su empleo en operaciones navales contemporáneas no solo mejora la conciencia situacional, sino que también permite anticipar amenazas, reducir incertidumbre táctica y exponer movimientos antes invisibles. Esta inteligencia permite trazar rutas, identificar puntos de reabastecimiento, detectar ejercicios navales o monitorear actividades portuarias en zonas disputadas.

Masters, J. (2024). Poder marítimo y política exterior de EE. UU. Council on Foreign Relations.

Un ejemplo paradigmático ha sido el conflicto en el **Mar Rojo entre 2023 y 2024**, donde el monitoreo público de los ataques hutíes a buques mercantes reveló un cambio táctico: se pudo rastrear qué embarcaciones eran seleccionadas como objetivos, cómo se modificaban sus rutas y en qué momentos se producían los lanzamientos. Grupos civiles y analistas de OSINT, empleando imágenes satelitales, datos AIS y publicaciones de redes sociales, lograron **mapear el patrón de amenazas y anticipar posibles zonas de riesgo** antes incluso que los sistemas oficiales de alerta marítima (Atlantic Council, 2024; NOSI, 2024).

CNN en Español. (2024). Secuestro de tripulación en el mar Rojo por hutíes. CNN en Español.

Otro caso ejemplar es el del **Mar Negro durante la guerra entre Rusia y Ucrania**. Analistas independientes utilizaron fuentes abiertas para identificar la presencia del crucero Moskva previo a su hundimiento en 2022, localizando su posición a través de imágenes satelitales y cambios en el tráfico marítimo circundante.

Más aún, el seguimiento de embarcaciones rusas encargadas del traslado de granos desde puertos ocupados se logró mediante OSINT marítimo, lo cual permitió denunciar en foros internacionales el saqueo de recursos ucranianos. Estas acciones tuvieron un impacto **táctico, político y legal**, exponiendo la actividad naval rusa incluso en zonas con fuerte censura mediática (Sutton, 2023).

Las herramientas más utilizadas en estos escenarios incluyen plataformas como **MarineTraffic**, **SkyTruth**, **Planet Labs**, **VesselFinder**, y bases de datos de registros navales y puertos. Complementadas con análisis de imágenes SAR (Radar de Apertura Sintética), permiten detectar embarcaciones incluso con AIS desactivado. Esta capacidad se convierte en una herramienta crítica para unidades navales de inteligencia, analistas de planeamiento táctico y centros de operaciones navales.

El uso táctico del OSINT también ha obligado a repensar los principios de **ocultamiento operacional**. Buques de guerra que operan en zonas de interés deben ahora considerar no solo la firma radar o térmica, sino también su **firma digital abierta**. Una publicación no oficial en Twitter, una imagen subida desde una playa, o la desactivación repentina del AIS, pueden alertar al adversario o incluso ser utilizadas como prueba en medios diplomáticos y jurídicos. La guerra naval moderna se libra, cada vez más, en el dominio de la información accesible.

Vulnerabilidades y contramedidas navales frente al OSINT.

El crecimiento exponencial de la Inteligencia de Fuentes Abiertas también ha generado **nuevas vulnerabilidades** para las fuerzas navales.

El principio tradicional de la "negación del conocimiento del adversario" se ve erosionado en un entorno donde **cualquier observador civil** armado con un teléfono satelital, acceso a internet y plataformas de geolocalización puede revelar información crítica sobre movimientos de buques, formaciones navales o patrones de abastecimiento.

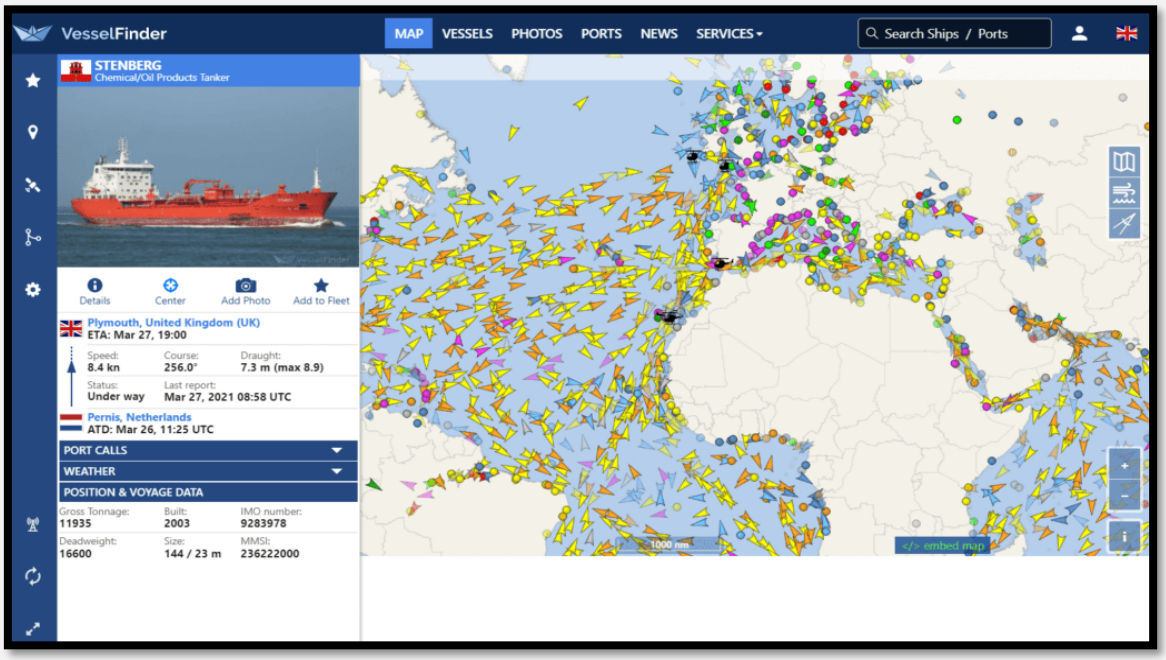
Entre las principales vulnerabilidades detectadas en operaciones recientes se encuentran: la exposición accidental a través de emisiones de AIS o dispositivos móviles, la identificación de

buques a partir de patrones de tráfico público, la detección de embarcaciones mediante imágenes satelitales comerciales, y la correlación de eventos en redes sociales que permiten anticipar operaciones navales encubiertas.

La guerra en Ucrania mostró casos en los que simples actualizaciones de aficionados marítimos permitieron localizar flotillas rusas en tránsito o prever bloqueos navales (Sutton, 2023).

Frente a esta amenaza, algunas marinas de guerra han comenzado a adoptar contramedidas específicas. La **gestión cuidadosa del AIS** (activaciones y desactivaciones bajo protocolos estrictos), el empleo de **señales de suplantación** o "spoofing", las maniobras tácticas diseñadas para **inducir a errores de interpretación en el tráfico abierto**, y el uso de **señuelos digitales** son algunas de las técnicas emergentes. Asimismo, entrenar a las dotaciones en "disciplina de la información", restringiendo publicaciones personales o comunicaciones no seguras, se ha convertido en un elemento fundamental del adiestramiento pre-operacional (Atlantic Council, 2024).

Paradójicamente, el propio uso de OSINT genera una **carrera de camuflaje e ilusión**: actores estatales y no estatales emplean fuentes abiertas para desinformar, simular despliegues, exagerar capacidades o distraer al adversario de operaciones reales. Así como el OSINT permite exponer vulnerabilidades, también puede ser instrumentalizado para **engañar y saturar** las capacidades analíticas del enemigo, generando "ruido" en el ciclo de inteligencia.



Lumper HQ. (s.f.). Mapa de tráfico marítimo en tiempo real. Lumper HQ.

Una dimensión particularmente interesante es que el OSINT, a diferencia de tecnologías sofisticadas como satélites de reconocimiento o redes SIGINT, **niveló en parte el acceso a capacidades de inteligencia**. Marinas más pequeñas, guardias costeras o incluso insurgencias navales han encontrado en el OSINT una **forma relativamente accesible de obtener conciencia situacional** frente a fuerzas superiores.

Esta democratización de la inteligencia plantea nuevos desafíos para la superioridad naval: **el control absoluto de la información en el mar es, cada vez más, una ilusión táctica**.

En síntesis, mientras que el OSINT expande el campo de observación, también obliga a repensar doctrinas de ocultamiento, disuasión, engaño y control de la firma digital en el entorno naval contemporáneo. El equilibrio entre aprovechar las ventajas del OSINT y protegerse de sus riesgos constituye hoy un factor decisivo en la preparación de fuerzas navales modernas.

Conclusiones, reflexiones y perspectivas finales.

El desarrollo exponencial de la Inteligencia de Fuentes Abiertas ha transformado la manera en que las fuerzas navales obtienen, procesan y actúan sobre la información. Lejos de ser un recurso marginal, el OSINT se ha consolidado como un insumo táctico y estratégico de alto valor, cuya accesibilidad, inmediatez y capacidad de contextualización ofrecen ventajas operacionales antes reservadas a potencias con superioridad tecnológica.

La integración del OSINT en operaciones navales modernas requiere más que plataformas digitales: exige doctrina, capacitación y una cultura institucional que valore la precisión, la verificación y el uso consciente de la información. Formar analistas capacitados en el procesamiento de datos abiertos, incluir módulos de OSINT en el planeamiento, y establecer protocolos claros de seguridad informacional son pasos ineludibles para reducir vulnerabilidades propias y maximizar el potencial de este recurso.

Además, resulta cada vez más evidente la necesidad de incluir perfiles técnicos mixtos —desde especialistas en sistemas geoespaciales hasta analistas con competencias en ciberseguridad o minería de datos— para abordar de forma integral los desafíos del dominio informacional abierto. Estas capacidades deben formar parte de la arquitectura de inteligencia naval junto a HUMINT, SIGINT y otras disciplinas tradicionales.

El OSINT también se presenta como un **multiplicador estratégico asimétrico**. Su bajo costo y su alta disponibilidad lo convierten en una herramienta clave para fuerzas que, sin disponer de medios de alta gama o satélites propios, pueden disputar información crítica y anticipar movimientos adversarios en escenarios navales complejos. En conflictos recientes, grupos no estatales e incluso pequeñas armadas han logrado generar conciencia situacional superior utilizando datos públicos, sensores comerciales y análisis colaborativo.

En este nuevo entorno, donde la exposición es constante y la información fluye en tiempo real, **la gestión activa del silencio, la negación digital, el camuflaje informacional y el engaño táctico se transforman en competencias tan relevantes como la maniobra, la detección o el fuego**. Navegar en el siglo XXI implica, también, maniobrar en el ciberespacio abierto.

Tactical Systems. (s.f.). Logo de Tactical OSINT Academy. Tactical OSINT Academy.

¿Hasta qué punto una fuerza con recursos limitados, pero con dominio del entorno informacional abierto, puede disputar superioridad táctica a una marina tecnológicamente más avanzada?

Tal vez la respuesta a esta pregunta defina no sólo el futuro del OSINT, sino también el modo en que concebimos la inteligencia, la táctica y la guerra en el mar.

Bibliografía.

- Atlantic Council. (2024). *Sailing through the spyglass: The strategic advantages of blue OSINT*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/sailing-through-the-spyglass-the-strategic-advantages-of-blue-osint-ubiquitous-sensor-networks-and-deception/
- Business Insider. (2024, julio). *Video shows an explosives-laden Jet Ski-style vehicle likely belonging to Ukraine*. https://www.businessinsider.com/ukrainian-military-jet-ski-explosives-istanbul-turkey-2024-7
- Ciberpatrulla. (s.f.). *Herramientas OSINT gratuitas*. https://ciberpatrulla.com/links/
- Díaz, A. (2016). *Las nuevas amenazas y los recursos del poder nacional* [Trabajo Final Integrador, CEFA]. CEFADigital. https://cefadigital.edu.ar/bitstream/1847939/894/1/TFI%2027-2016%20RIQUELME.pdf
- De Gruyter Brill. (2023). *Open-source intelligence in the Russia–Ukraine war: Tactical impacts and challenges*. https://www.degruyterbrill.com/document/doi/10.24415/9789400604742-005/html
- EOS Data Analytics. (s.f.). *Imágenes de satélite gratis: los mejores proveedores*. https://eos.com/es/blog/imagenes-de-satelite-gratis/
- Defense Intelligence Agency. (2024). *Open Source Intelligence Strategy 2024–2028*. https://www.dia.mil/Portals/110/Documents/OSINT-Strategy.pdf
- Geekflare. (2024). *Las mejores herramientas OSINT para ciberinvestigaciones*. https://geekflare.com/es/osint-tools/

LISAINSTITUTE. (s.f.). *Inteligencia de fuentes abiertas (OSINT): tipos, métodos y salidas profesionales*. https://www.lisainstitute.com/blogs/blog/osint-inteligencia-fuentes-abiertas

- MarineTraffic. (2024). *Global ship tracking intelligence platform*. https://www.marinetraffic.com/en/ais/home/centerx:-12.0/centery:25.0/zoom:4
- NOSI – Naval Open Source Intelligence. (2024). *Houthi Navy Activity Reports*. https://nosi.org/category/houthinavy/
- Planet Labs. (2024). *Daily satellite imagery and analytics platform*. https://www.planet.com/
- Reuters. (2024, enero 17). *Business heads see Red Sea tensions causing lengthy trade dislocation*. https://www.reuters.com/business/business-heads-see-red-sea-tensions-causing-lengthy-trade-dislocation-2024-01-17/
- Riquelme, A. (2019). *El uso de la inteligencia de fuentes abiertas como elemento de apoyo a la seguridad nacional* [Trabajo de curso, CEFA]. CEFADigital. https://cefadigital.edu.ar/bitstream/1847939/1335/1/VC%2021-%202019%20Casarino-Ortiz.pdf
- Sutton, H. I. (2023). *Reflecting on one year of war: The power of open-source intelligence*. Center for Maritime Strategy. https://centerformaritimestrategy.org/publications/reflecting-on-one-year-of-war-the-power-of-open-source-intelligence/
- Authentic8. (2023). *Maritime OSINT: Tips, tools & techniques*. https://www.authentic8.com/blog/maritime-osint-rae-baker
- Univision Noticias. (2023, octubre 7). *Qué es OSINT y por qué ese trabajo es tan importante en tiempos de guerra*. https://www.univision.com/noticias/cronicas-desinformacion-osint-importante-tiempos-guerra
- VesselFinder. (2024). *Live ship tracking and maritime intelligence*. https://www.vesselfinder.com/
- WeLiveSecurity. (2023, febrero 28). *5 herramientas OSINT gratuitas para redes sociales*. https://www.welivesecurity.com/la-es/2023/02/28/5-herramientas-osint-gratuitas-redes-sociales/

- Frontiers in Computer Science. (2023). *Shining a light on AIS blackouts with maritime OSINT*. https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2023.1185760/full
- OSINT Argentina. (s.f.). *Noticias y análisis sobre inteligencia de fuentes abiertas*. https://osint.com.ar/
- Knowlesys. (s.f.). *La mejor guía para el marco OSINT*. Knowlesys OSINT Academy. https://knowlesys.com/es/osint-academy/analytics/the-ultimate-guide-to-the-osint-framework.html
- Nitti, M. E., Riedlbauer, D., & Li, L. (2024, agosto 7). *OSINT Toolkit: MarineTraffic, a Real-Time Vessel Tracking Tool That Enhances Maritime Security and Verifies Naval Operations During Critical Situations*. The Counterterrorism Group. https://www.counterterrorismgroup.com/post/osint-toolkit-marinetraffic-a-real-time-vessel-tracking-tool-that-enhances-maritime-security-and-v
- Lumper HQ. (s.f.). *Live Marine Traffic Map*. https://lumperhq.com/live-marine-traffic-map/
- Masters, J. (2024, junio 12). *Sea Power: The U.S. Navy and Foreign Policy*. Council on Foreign Relations. https://www.cfr.org/backgrounder/sea-power-us-navy-and-foreign-policy
- CNN en Español. (2024, marzo 15). *La historia de la tripulación olvidada del conflicto de Gaza que los hutíes mantienen como rehenes en el mar Rojo*. CNN en Español. https://cnnespanol.cnn.com/2024/03/15/tripulacion-huties-rehenes-mar-rojo-buque-trax
- Tactical Systems. (s.f.). *Tactical OSINT Academy*. https://www.tactical-osint-academy.com/

» Batalla de Jutlandia I

Por CN (RE) Prof. Lic. Guillermo Spinelli [15]

Situación:

La Primera Guerra Mundial inicia el 28 de julio de 1914 y se prolongará por cuatro largos años. Este conflicto se caracterizó por el inmovilismo de las posiciones, especialmente en el frente occidental, que rápidamente se convirtió en un frente de trincheras. A esto se sumó el bloqueo impuesto por la Royal Navy, que redujo drásticamente las posibilidades de abastecimiento de los Imperios Centrales.

Tras la batalla del Banco de Dogger en enero de 1915, en la que se impuso el Imperio Británico, las acciones navales quedaron paralizadas hasta mediados de ese año, cuando los submarinos alemanes lograron contrarrestar parcialmente el bloqueo inglés, inaugurando una guerra total que incluyó el ataque a buques comerciales sin restricciones. Sin embargo, esta estrategia fue revisada debido a la presión diplomática de los países neutrales.

Este cambio estratégico fue cuestionado por el nuevo jefe de la Flota de Alta Mar alemana, el almirante Reinhard Scheer, quien proponía un uso más agresivo de la flota, combinando buques de guerra, submarinos y zepelines para reducir la superioridad numérica inglesa.

Tecnología de la época

Flotas y buques:
La construcción naval había avanzado significativamente, dando lugar a distintos tipos de buques diseñados para maximizar el uso de las nuevas armas. Algunos de los principales eran:

[15] Capitán de Navío (RE), profesor y licenciado en historia. Secretario de Extensión y Vinculación Universitaria de la Facultad de la Armada (FadARA).

- Acorazados:
  Descendientes directos de los antiguos buques de línea, los primeros acorazados eran versiones mejoradas de estos, con corazas y propulsión a vapor. En 1906, la Royal Navy botó el HMS *Dreadnought*, un buque que revolucionó la construcción naval, dejando obsoletos a los modelos anteriores. Las potencias navales se enfocaron en construir este tipo de buques, caracterizados por una batería homogénea de calibres que variaban entre 11 y 15 pulgadas (280-381 mm) y velocidades de 20 a 26 nudos.

- Cruceros de batalla:
  Mejorados a partir de los cruceros acorazados, estos buques combinaban características de los *Dreadnoughts*, con tamaño y armamento similares a los acorazados, pero con menor blindaje, lo que les otorgaba mayor velocidad. Eran especialmente útiles para exploración.

- Cruceros ligeros:
  Evolucionaron de los cruceros protegidos. Contaban con armamento de calibre promedio de 152 mm y una protección ligera, y se empleaban principalmente para exploración y apoyo en ataques de destructores.

- Destructores y torpederos:
  Los torpederos eran buques rápidos diseñados para atacar con torpedos. Su desplazamiento rondaba las 1.000 toneladas. Por su parte, los destructores estaban equipados con artillería más potente para defender a los buques capitales de ataques torpederos. Estos operaban en flotillas que se desplazaban rápidamente para lanzar una salva de torpedos a corta distancia.

El tiro de artillería a larga distancia

Con el desarrollo de los cañones de largo alcance, se hizo necesario un sistema que permitiera impactos precisos a grandes distancias. Este debía resolver varios factores, como:

1. Determinar la posición actual del blanco.
2. Predecir la posición futura del blanco y calcular los ángulos de adelanto.
3. Estabilizar las plataformas de tiro ante los efectos del balance y cabeceo del buque.
4. Calcular las correcciones necesarias para la orientación y elevación de los cañones.
5. Transmitir órdenes precisas a las baterías.
6. Realizar el *spotting*, es decir, observar los piques de los disparos para ajustar el tiro.

Balística externa básica:
Al disparar sobre un blanco a más de 12.000 yardas, varios factores influían en la trayectoria del proyectil, causando variaciones incluso dentro de la misma salva. Estas diferencias, como velocidades relativas o cambios de rumbo, requerían correcciones constantes para lograr impactos.

Se utilizaban salvas de artillería, disparos simultáneos de varios cañones. El patrón de impacto formaba una "rosa de tiro", cuyo centro debía coincidir con el blanco. Las correcciones se realizaban con base en las observaciones de los piques, ajustando deflexión y elevación.

Sistema de control de tiro alemán

Los cañones eran controlados desde una central ubicada en lo alto de los buques para garantizar una mejor visibilidad del blanco. Había al menos dos de estas centrales para prevenir fallos por daños.

El sistema estaba conectado por teléfono, tubos neumáticos y transmisiones eléctricas. La distancia al blanco se calculaba mediante telémetros ópticos estereoscópicos, y los datos se procesaban en una computadora mecánica basada en el dispositivo de cálculo inventado en 1902 por el teniente inglés Dumaresq. Este instrumento calculaba el rumbo y velocidad relativa del enemigo, permitiendo apuntar con precisión.

Comparación entre sistemas

El sistema alemán era más simple e integrado, mientras que el inglés era más robusto pero complicado. Los telémetros estereoscópicos alemanes ofrecían mayor precisión y sus operadores estaban mejor entrenados.

Impacto de la tecnología en la táctica

El alcance y la precisión de las armas cambiaron las dinámicas del combate naval, que se desarrollaba a más de 10.000 yardas con cañones de gran calibre. La superioridad del cañón sobre el blindaje obligó a diseñar buques más ligeros, protegidos principalmente en áreas críticas como torres de artillería y depósitos de municiones.

El torpedo, por su parte, permitió que buques pequeños como torpederos y destructores infligieran daños significativos, obligando a los acorazados a desarrollar baterías secundarias para protegerse.

Tácticas

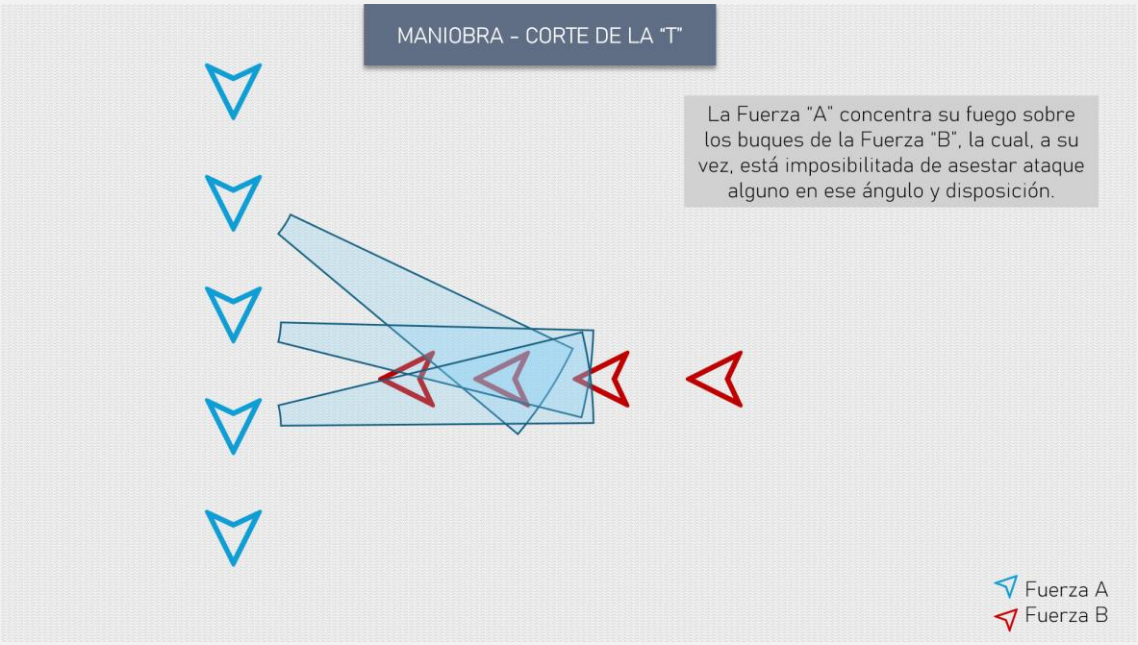
La formación en columna se consideraba la más efectiva para el combate, ya que permitía concentrar el fuego sobre el enemigo. Para navegar hacia la batalla, las flotas adoptaban formaciones divididas en columnas menores, reorganizándose en una sola columna al entrar en combate.

En resumen, la batalla de Jutlandia mostró cómo la tecnología y las tácticas evolucionaron durante la Primera Guerra Mundial, marcando un punto de inflexión en la guerra naval.

En el caso germano, la formación tanto para la navegación de crucero como para el combate era la columna, ya que, al contar con una menor cantidad de acorazados, esta resultaba la táctica más adecuada.

Dado que la transición entre la navegación de crucero y la disposición en columna para el combate requería un tiempo considerable, se utilizaba un grupo de exploración posicionado al frente, a una distancia de entre 20 y 30 millas. Este grupo tenía como objetivo brindar al grueso de la flota la oportunidad de formarse y posicionarse estratégicamente.

Aunque las flotas combatían en columna, ambas buscaban realizar la maniobra conocida como "cortar la T". Esto consistía en colocar la propia columna en un ángulo de noventa grados respecto a la del adversario, logrando concentrar el fuego sobre la cabeza de la columna enemiga. Esta posición dejaba a los buques delanteros de la flota rival en desventaja, ya que dificultaban la capacidad de los barcos ubicados detrás para responder eficazmente al ataque.



Es interesante destacar que la Flota de Alta Mar germana había previsto cómo actuar si su columna quedaba expuesta a la maniobra de "cortar la T". La estrategia consistía en realizar un giro simultáneo de la línea de batalla hacia el rumbo opuesto, una maniobra previamente ensayada y definida, especificando la banda por la que se efectuaría. Este procedimiento comenzaba con el buque de popa, que giraba 180° hacia su rumbo opuesto, seguido por el resto de los buques en orden progresivo hacia proa. La maniobra, aunque eficaz, era extremadamente compleja y conllevaba un riesgo real de colisión, un peligro que se incrementaba significativamente al ejecutarse en condiciones de combate o con baja visibilidad. Durante la batalla que nos ocupa, esta maniobra se llevó a cabo bajo ambas condiciones simultáneamente. La línea de batalla, con una longitud de entre 6 y 8 millas, enfrentaba la posibilidad de confusión o retrasos, lo que podría haber resultado en abordajes entre los acorazados.

Fuerzas enfrentadas:
Comandantes:
John Jellicoe: comandante de la *Grand Fleet* en Jutlandia. Su forma de combatir era conocida, ya que había informado previamente a la flota sobre sus intenciones. Era consciente de que el peso de una posible derrota superaba el de una victoria, así como del estado general de la flota bajo su mando y de la superioridad cualitativa de la flota germana. Aunque maniobró con acierto, fue criticado por falta de agresividad y, en consecuencia, responsabilizado del pobre resultado táctico de la batalla. Posteriormente, sería reemplazado por Rosslyn Wemyss y luego por su detractor, David Beatty.

David Beatty: comandante de la fuerza de exploración de la *Grand Fleet* en Jutlandia. De carácter agresivo e impulsivo, cometió varios errores en sus enfrentamientos. En la batalla del Banco Dogger, ordenó concentrar el ataque sobre la retaguardia enemiga, permitiendo la huida del resto del escuadrón alemán. En Jutlandia, pese a contar con superioridad numérica, perdió dos cruceros de batalla debido a su manejo deficiente de las fuerzas. Además, no informó correctamente a su superior sobre las fuerzas enemigas, incumpliendo su principal tarea como líder de las fuerzas de exploración.

Reinhard Scheer: comandante de la Flota de Alta Mar alemana desde enero de 1916, tras sustituir al almirante Hugo von Pohl, a quien criticó por falta de agresividad. Scheer intentó integrar los zepelines y submarinos para desgastar a la *Grand Fleet* y equilibrar las fuerzas. Maniobró su flota con habilidad, logrando extraerla de situaciones extremadamente comprometidas en dos ocasiones.

Franz von Hipper: comandante de las fuerzas de exploración de la flota alemana. Era un hombre valiente y dedicado que maniobró su fuerza, claramente inferior, con gran habilidad. Combatió con coraje y cumplió su deber de informar a su superior sobre las fuerzas enemigas. A pesar de la inferioridad numérica, infligió un daño significativo a su oponente.

Personal:
Las dotaciones de ambas flotas eran similares, aunque el adiestramiento alemán era más intenso y realista. Los telemetristas alemanes obtuvieron excelentes resultados durante la batalla, superando a sus homólogos ingleses. Ambas fuerzas combatieron con valentía y entregaron lo mejor de sí mismas.

Material:
Flota inglesa:
Primer Escuadrón de Batalla

A esta fuerza se le agrega: 8 cruceros acorazados.

- 26 cruceros ligeros
- 78 destructores
- 1 buque minador
- 1 buque portahidroaviones

Flota de Alta Mar - Se agregan:

- 11 cruceros ligeros
- 61 torpederos

Cañones totales ingleses	328
Cañones totales Flota de Alta Mar	248

C3

En ese período histórico, el comando de una flota se llevaba a cabo mediante diferentes medios: visuales y radiofónicos. Entre los primeros se encontraban las señales con banderas y focos, mientras que la comunicación inalámbrica representaba una innovación tecnológica. En este último aspecto, los alemanes contaban con una marcada superioridad gracias a equipos más modernos y eficaces. Sin embargo, el caso germano resulta paradigmático, ya que la radio fue tanto su fortaleza como su debilidad.

Como fortaleza, cabe destacar su gran capacidad táctica, incluso en situaciones peligrosas, como las dos ocasiones en que se realizó el giro de combate. Por otro lado, como debilidad, es importante mencionar que el "cuarto 40" inglés interceptó las comunicaciones radiales alemanas, permitiendo a la flota británica zarpar antes que la alemana. Scheer, quien pretendía sorprender a una parte de la flota inglesa y enfrentarse a ella en condiciones de ventaja numérica frente a la superior *Home Fleet*, terminó siendo él mismo el sorprendido debido al mal uso de las comunicaciones inalámbricas por parte de los alemanes y al excelente manejo de estas por el almirantazgo inglés.

Ambos estilos de comando eran similares, aunque presentaban diferencias notables. En el caso alemán, el mando era más descentralizado, ya que el almirante Scheer confiaba en el intensivo adiestramiento de sus subordinados. En contraste, Jellicoe tendía a centralizar su comando, motivado por la necesidad de mantener su flota en una formación compacta y masificada, con el objetivo de evitar que una parte de esta se viera obligada a enfrentarse sola contra la totalidad de la flota alemana.

Debido a la gran cantidad de buques involucrados, así como a las complejidades cinemáticas y meteorológicas, el sistema de comando, control y comunicaciones (C3) se llevó al límite, lo que ocasionó errores y malinterpretaciones de órdenes.

Modelo de la batalla

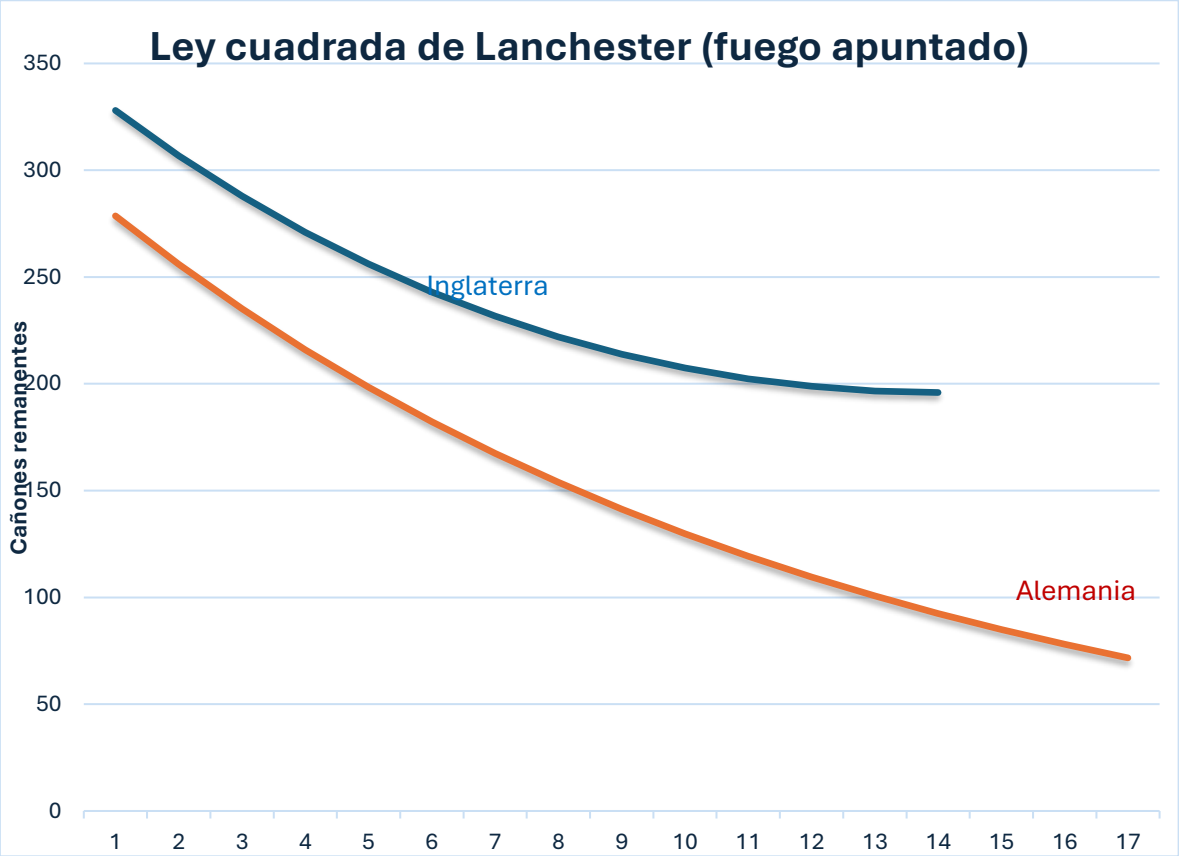
En la primera imagen se representa el desgaste mutuo en caso de enfrentamiento directo entre ambas líneas de batalla.

Datos:

- **Número de cañones ingleses:** 328
- **Número de cañones alemanes:** 248
- **Coeficiente de letalidad inglés:** 0,8

- **Coeficiente de letalidad alemán:** 0,9

En este primer gráfico se simula el enfrentamiento total de ambas flotas, incorporando una ligera ventaja cualitativa a favor de Alemania.

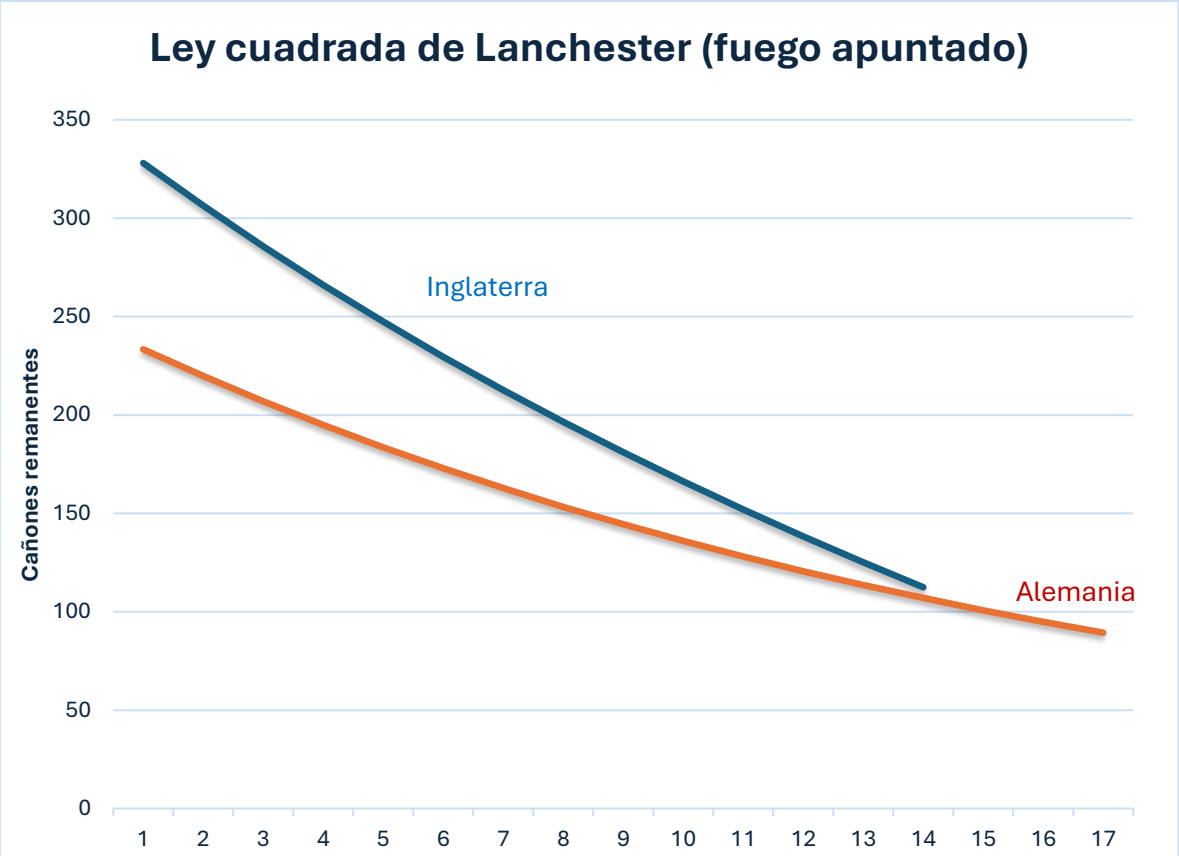


Se observa que la flota alemana pierde su capacidad de combate más rápidamente que la inglesa, a pesar de contar con una ligera ventaja en calidad (coeficiente de letalidad 0,9 para la flota alemana frente a 0,8 para la inglesa). Esta desventaja progresiva lleva a una eventual derrota. Para el tiempo 14, la flota alemana conserva aproximadamente 80 cañones de un total inicial de 248 (una pérdida de 168 cañones), mientras que la flota inglesa retiene 200 cañones de sus 328 iniciales (una pérdida de 128 cañones). Se puede observar que la pendiente de disminución de la capacidad inglesa es más moderada, mientras que la alemana se vuelve más pronunciada. Este análisis demuestra cómo la cantidad prevalece sobre la calidad en este escenario.

En este segundo caso, se modifica el factor calidad (coeficiente de letalidad):

Datos:

- **Número de cañones ingleses:** 328
- **Número de cañones alemanes:** 248
- **Coeficiente de letalidad inglés:** 0,4
- **Coeficiente de letalidad alemán:** 0,9



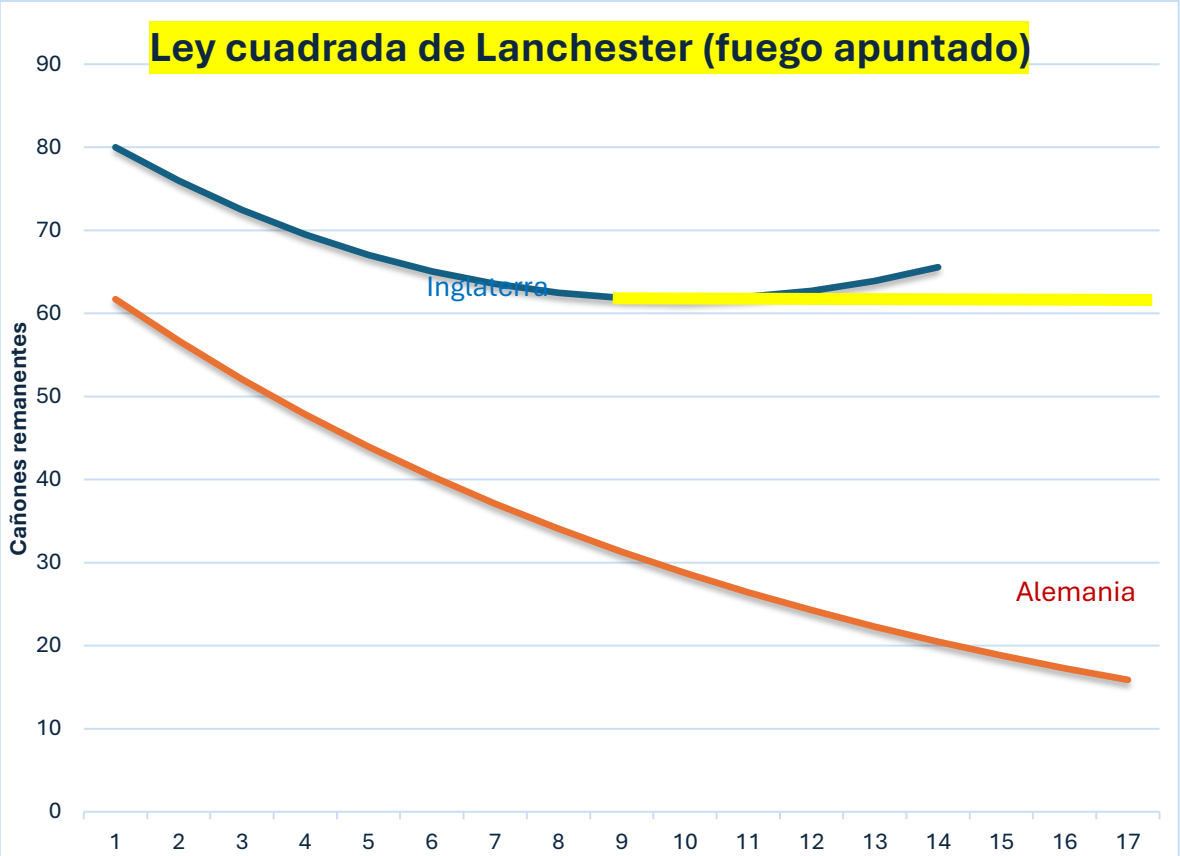
Se observa que, aunque la flota alemana muestra una calidad más del doble superior a la inglesa (un escenario poco probable), logra reducir sus pérdidas pero no alcanza a superar numéricamente a la flota combinada dentro del marco temporal graficado. Aunque los alemanes hicieron un esfuerzo significativo por superar cualitativamente a los ingleses, dado que no podían igualarlos cuantitativamente, resulta improbable considerar que su calidad fuera más del doble. Esto se debe a que, aunque sus buques eran muy resistentes, también eran más lentos, y aunque su artillería era de excelente calidad, era de menor calibre.

De las comparaciones realizadas se concluye que la cantidad tiene un peso mayor que la calidad.

Análisis del encuentro entre las fuerzas de exploración:

Datos:

- Número de cañones ingleses: 80
    - Grupo de Exploración (Beatty): 48
    - Quinta Escuadra de Batalla de Evan-Thomas: 32
- Número de cañones alemanes: 48
    - Grupo de Exploración (Hipper): 48
- Coeficiente de letalidad inglés: 0,7
- Coeficiente de letalidad alemán: 0,9

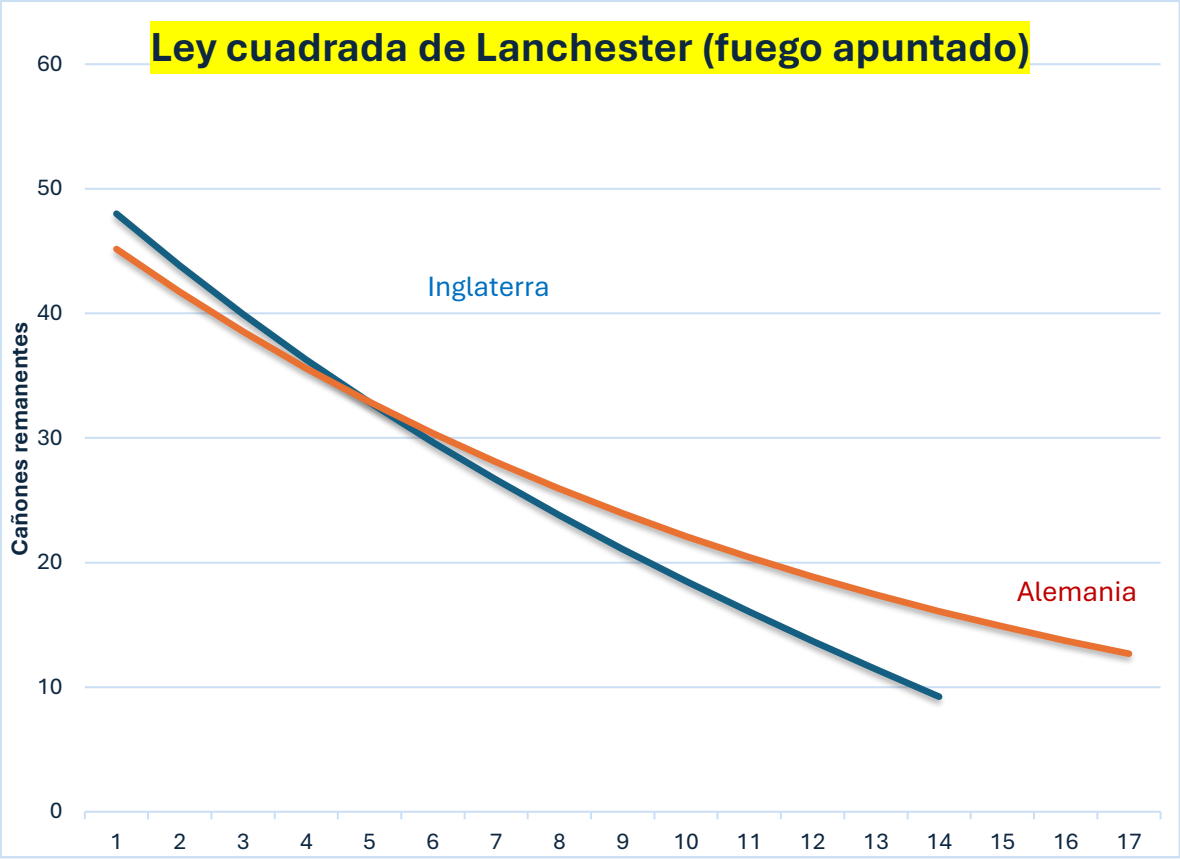


El encuentro entre las fuerzas de exploración, comandadas por los almirantes Beatty y Hipper, respectivamente, debería haberse desarrollado de manera equilibrada. Sin embargo, la precipitada aproximación de Beatty y la falta de iniciativa de Evan-Thomas apartaron de la fuerza inglesa a la poderosa Quinta Escuadra de Batalla, lo que le restó 32 cañones de gran calibre (381 mm, los mayores empleados en ambas fuerzas durante la batalla). Esta situación debilitó significativamente la posición inglesa.

Pese a ello, la ventaja inicial de Beatty sigue siendo evidente.

Datos:

- Número de cañones del Grupo de Exploración (Beatty): 48
- Número de cañones del Grupo de Exploración (Hipper): 48
- Coeficiente de letalidad inglés: 0,7
- Coeficiente de letalidad alemán: 0,9



La incorrecta aproximación de Beatty, quien dejó muy atrás a Evan-Thomas, y la falta de esfuerzo de este último por acortar distancias provocaron graves pérdidas en el grupo de exploración inglés.

Beatty, al aproximarse, ejecutó numerosas maniobras y emitió un elevado volumen de comunicaciones mediante foco y banderas, pero sin dejar claras sus intenciones. Incluso ordenó a Evan-Thomas navegar en un rumbo específico, cuando lo más adecuado habría sido informarle sobre sus planes y permitirle actuar en consecuencia. Sus maniobras resultaron complicadas y poco comprensibles.

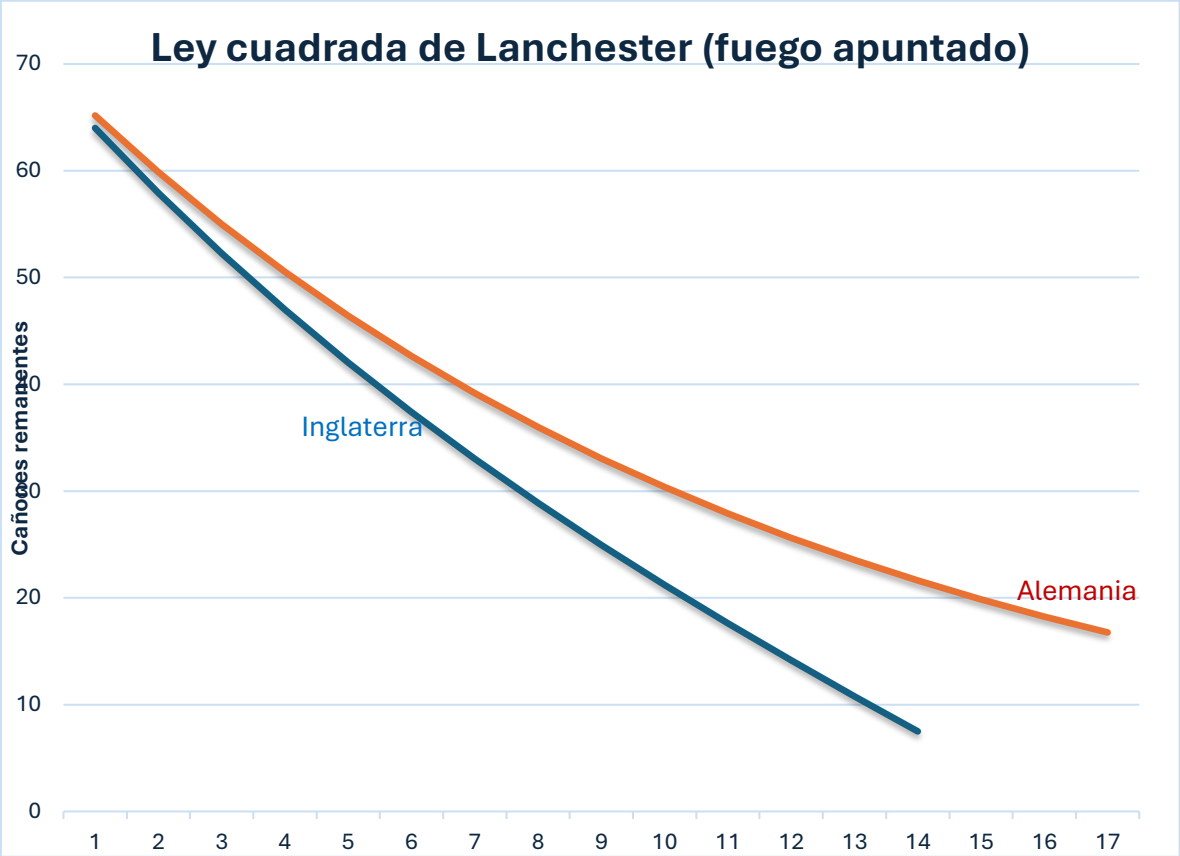
Por el contrario, el Grupo de Exploración alemán se impuso inicialmente gracias a un comando más efectivo. Sin embargo, este triunfo fue breve, ya que la incorporación de la Quinta Escuadra de Batalla de Evan-Thomas inclinó la balanza debido a la desproporción numérica. En ese nuevo escenario, la situación se tornó crítica para Hipper: sus buques estaban averiados y se enfrentaban a una fuerza numéricamente superior, a pesar de la brillante actuación alemana.

A continuación, se modelará el ingreso en combate de la Flota de Alta Mar.

Datos:

- **Número de cañones del Grupo de Exploración (Beatty):** 64 (se suma la Quinta Escuadra de Batalla de Evan-Thomas y se restan los cañones del *Queen Mary* y el *Indefatigable*, ya hundidos).
- **Número de cañones del Grupo de Exploración (Hipper):** 40 (se resta el *Von der Tann*, que permanecía operativo, pero con su artillería completamente fuera de servicio. Se suman 30 cañones de los acorazados que alcanzaron a disparar sobre los buques de Beatty antes de que este rompiera contacto y se replegara hacia su flota).
- **Coeficiente de letalidad inglés:** 0,7

- **Coeficiente de letalidad alemán:** 0,9

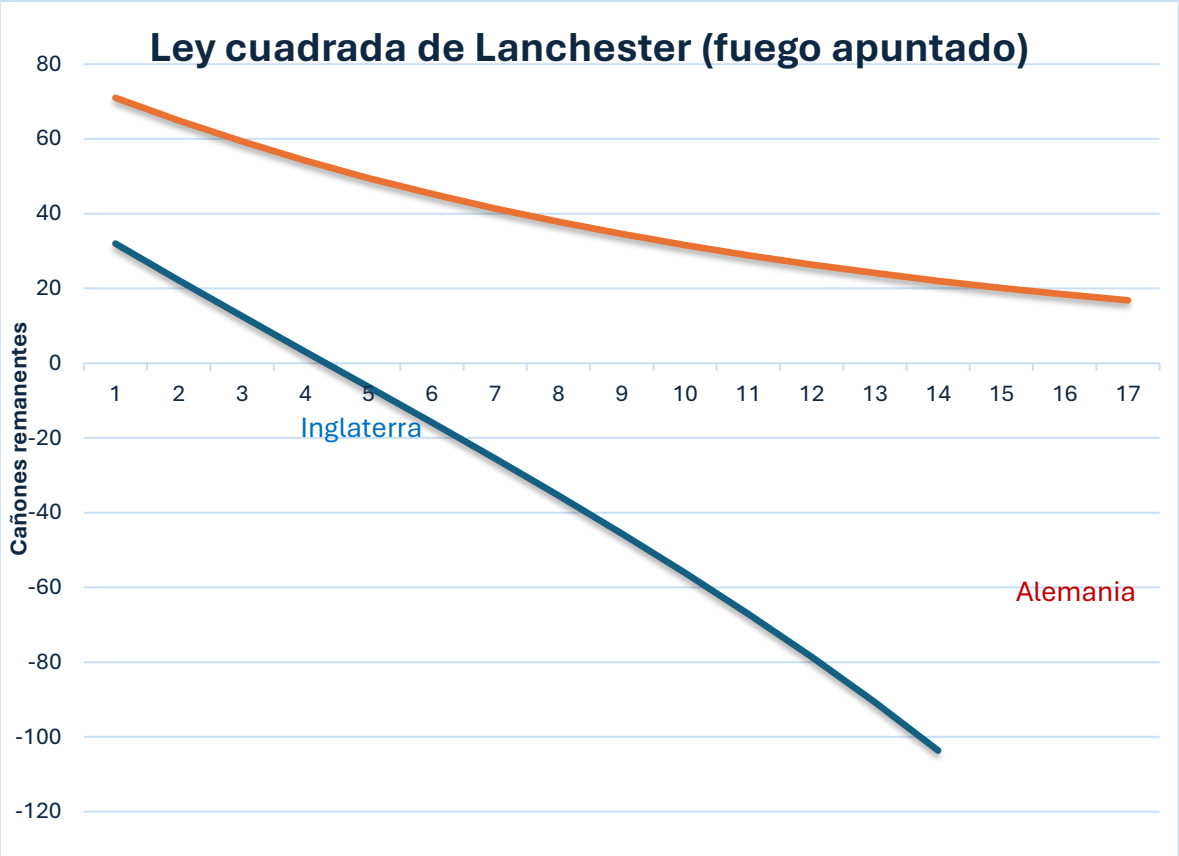


Como se observa, el encuentro era completamente desfavorable para Beatty, quien actuó acertadamente al retirarse hacia su propia flota. Este movimiento tenía un doble propósito: protegerse y atraer a la flota alemana hacia la **Home Fleet**.

Sin embargo, una vez más, Beatty cometió un error. Evan-Thomas lo siguió rezagado, exponiéndose al fuego del grueso alemán antes de poder incorporarse plenamente a la maniobra de repliegue.

Datos:

- **Número de cañones ingleses:** 32
- **Número de cañones alemanes:** 110
- **Coeficiente de letalidad inglés:** 0,9
- **Coeficiente de letalidad alemán:** 0,9



El error de Beatty pudo haber conducido a un desastre para la Quinta Escuadra de Evan-Thomas. Sin embargo, esto no ocurrió debido a la mala visibilidad y a la falta de tiempo para concretar el resultado. El grupo de exploración alemán fue poco efectivo, afectado por el cansancio y las bajas sufridas. A esto se sumaba que la distancia de enfrentamiento era considerable.

» Desafío Táctico del OTN

Al lector

Situación: En los últimos meses, la Flota del Mar Negro ha sido objeto de ataques reiterados con USVs (vehículos de superficie no tripulados) por parte de fuerzas ucranianas, tanto en aguas abiertas como dentro del puerto de Sebastopol.

El desafío: Póngase en el lugar del Jefe de Operaciones ruso. ¿Qué medidas tácticas, tecnológicas o doctrinales adoptaría para neutralizar esta amenaza?

Piense en recursos disponibles, limitaciones del entorno, capacidades del enemigo y posibles innovaciones.

🧭 **Su respuesta puede ser publicada en el próximo boletín.**

📲 **Enviee su respuesta a extension@fa.undef.edu.ar con el asunto "Desafío Táctico MAY 25"; tiene tiempo hasta el 31 JUN 25.**

» Acerca del Observatorio de Táctica Naval:

Fundado en 2024, en el marco de la Escuela de Oficiales de la Armada, de la Facultad de la Armada, por iniciativa de un grupo de oficiales de la Armada Argentina interesados en profundizar en las novedades sobre los desarrollos tecnológicos y tácticos navales.

» ¡El OTN te está buscando!

Si tenés interés en participar del Observatorio podés escribirnos a extension@fa.undef.edu.ar con tu CV y un tema en el cual deseas realizar tus aportes, relacionado con escenarios donde se manifiesten las innovaciones y cambios en la táctica naval, actuales o en clave histórica.