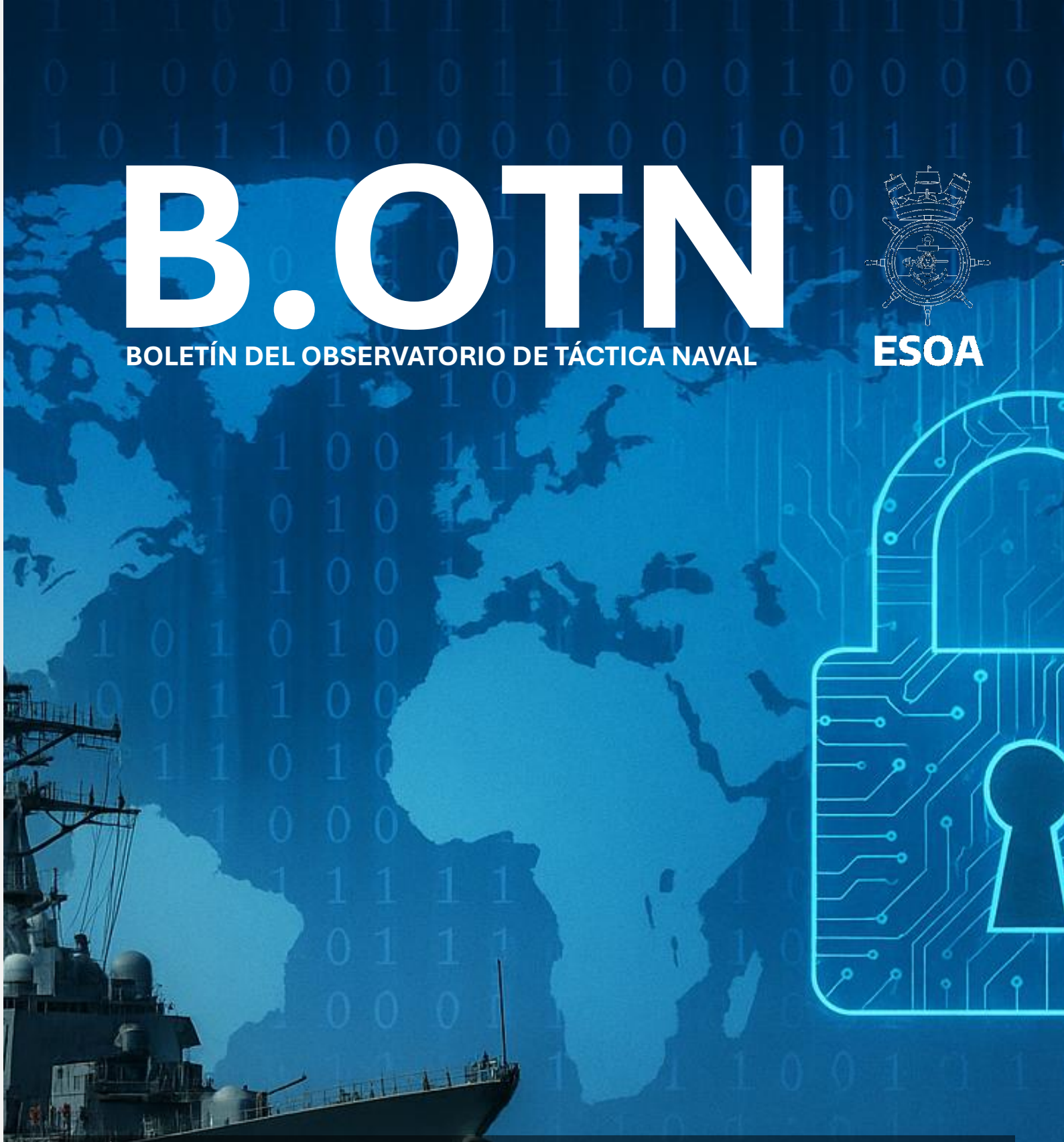
B.OTN

BOLETÍN DEL OBSERVATORIO DE TÁCTICA NAVAL

ESOA



Número Especial: capacidades navales en escenarios complejos: comercio, logística y el desafío del escenario cibernético

FadARA
Facultad de la Armada

OCTUBRE
2025

ISSN 3072-7820

» Autoridades

Director General de Educación de la Armada

CL Lic. Contralmirante Juan Carlos Romay

Decano de la Facultad de la Armada

CN (RE) Lic. Gonzalo Hernán Prieto

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

ISSN 3072-7820

Todos los derechos reservados. Distribución gratuita. Prohibida su venta. No se permite la reproducción total o parcial de este libro, su almacenamiento en un sistema informático, su transmisión en cualquier forma, o por cualquier medio, electrónico, mecánico, fotocopia u otros métodos, sin previa autorización de los autores y del Equipo Editorial.

Contenido

» Bienvenidos

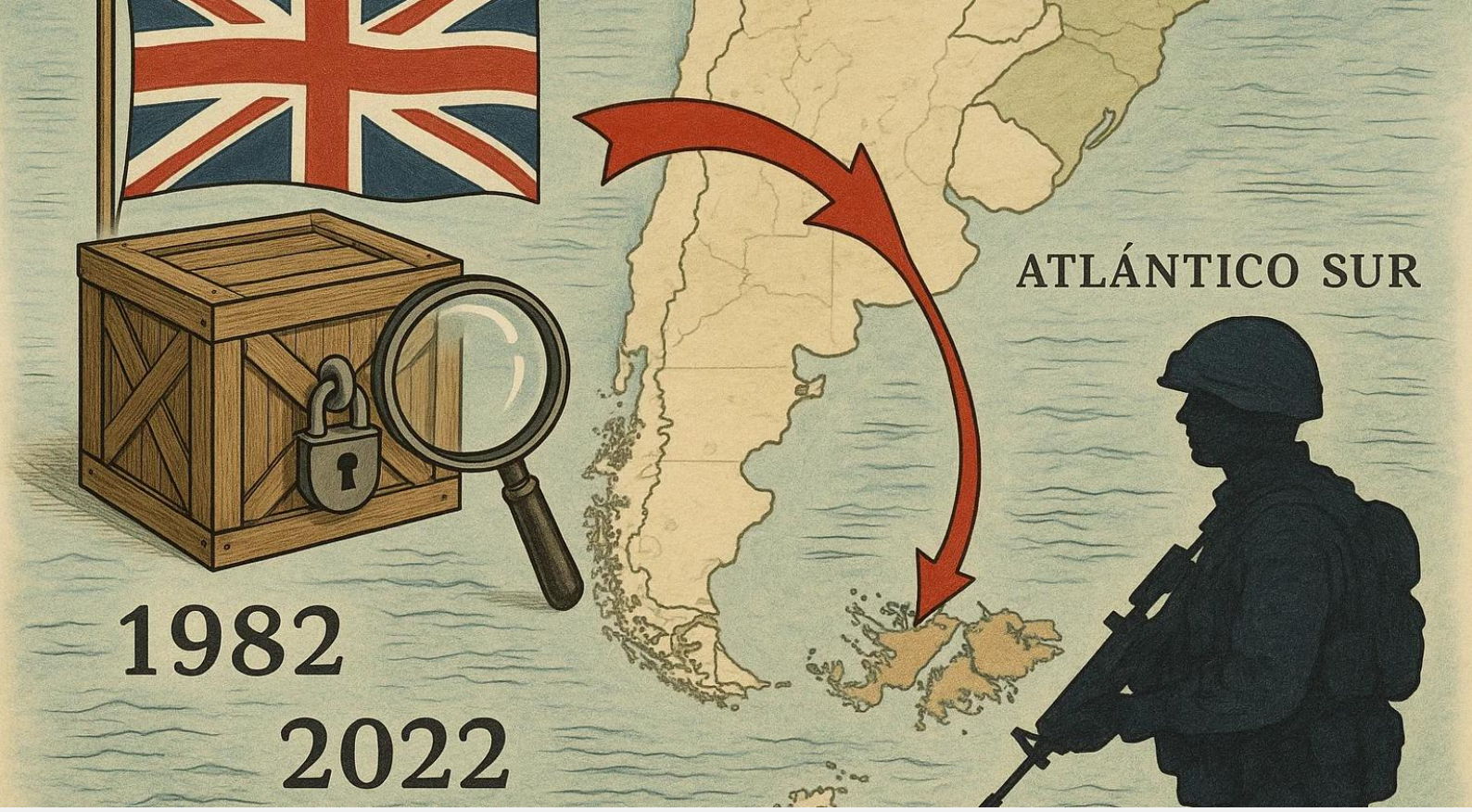
Por Prof. Mg. Eugenio Koutsovitis [1]

El Boletín del Observatorio de Táctica Naval llega a un pequeño gran hito, el quinto número con excelentes trabajos dedicados al desafío del escenario cibernético en el despliegue de capacidades navales. Este volumen reúne una visión integral y actualizada sobre los desafíos que enfrenta la táctica naval en la era digital, con un enfoque transversal en la ciberseguridad y la transformación tecnológica de las fuerzas marítimas. A lo largo de sus artículos, el boletín explora cómo la digitalización, la automatización y la interconexión global han redefinido tanto las amenazas como las oportunidades para la defensa naval.

El compendio aborda, de manera articulada, la importancia de proteger infraestructuras críticas marítimas frente a riesgos híbridos y cibernéticos, la necesidad de incorporar modelos computacionales y simulaciones para el planeamiento y la toma de decisiones, y el impacto de las políticas geopolíticas en la capacidad militar nacional. Se profundiza en la comprensión del ciberespacio como un nuevo dominio de conflicto, analizando tanto la naturaleza de la ciberguerra como la integración de operaciones ofensivas y defensivas en el ámbito digital.

Además, se destaca la relevancia de la concienciación y la formación en ciberseguridad para preservar el poder de combate, así como la adaptación doctrinaria de los principios clásicos de la guerra a los escenarios virtuales. El boletín también examina casos recientes y lecciones aprendidas, subrayando la necesidad de resiliencia, cooperación y actualización constante frente a un entorno cada vez más complejo y dinámico.

[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.



» La política de control de exportaciones británica como instrumento geopolítico en el Atlántico Sur (1982-2022)

Por Lic. Florencia Mendieta [2]

El Atlántico Sur ha adquirido creciente relevancia estratégica, siendo las Islas Malvinas un punto clave tanto para Argentina como para otros actores internacionales. Desde 1982, el Reino Unido mantiene un embargo de armas sobre Argentina como parte de su política de defensa y control de exportaciones, limitando el desarrollo militar argentino y consolidando su presencia estratégica en la región. Este trabajo se propone analizar la política británica de control de exportaciones y la militarización del Atlántico Sur entre 1982 y 2022, evaluando su impacto sobre la defensa argentina.

"Conflicto del Atlántico Sur: Aspiraciones de los actores intervinientes"

De acuerdo a Marini (1980), la geopolítica es la ciencia que estudia las mutuas relaciones, influencias y acciones entre el Estado y el espacio, a fin de aportar conocimientos o soluciones de carácter político. En el "espacio geopolítico" actúan recíprocamente los factores geográficos y políticos que conforman una situación geopolítica que se desea estudiar o resolver (p. 25), siendo el espacio estratégico, un objeto que se le otorga cierto valor, denotando la existencia de intereses. Es así que "Malvinas es un pedazo de tierra; pero, bajo la visión de la integridad territorial argentina, ese objeto cobra máximo valor y se convierte en un interés, porque la soberanía es un interés vital. El problema es que, en el mismo escenario, el Atlántico sur y la Antártida, hay otros actores que también le otorgan máximo valor a ese objeto y lo convierten en su interés. De esa competencia surge la actual dialéctica de voluntades en conflicto" (Nogueira, 2022, p. 11). De manera que los

[2] Licenciada en Relaciones Internacionales (UNLA). Docente asistente en UNLA. Este artículo pertenece a un estudio más amplio (Trabajo Final Integrador): "Causas y efectos de la política de control de exportaciones estratégicas británica aplicada a Argentina (1982-2022)", el cual contempla un análisis prospectivo. Email: Florenciamendietaunla@gmail.com

factores políticos permanecen relacionados con la interpretación política que se realiza de la información ofrecida por los factores geográficos, para que el espacio interese a la geopolítica, este debe tener significación política, una relación o un sentido para el Estado (Marini, 1980). En el presente caso, existe relación superpuesta entre "comunión espacio-Estado" que generó una interpretación política distinta entre Argentina y otros actores, plasmandose en el Conflicto del Atlántico Sur.

Autores afirman que la guerra fue planificada por el Reino Unido y Estados Unidos, influyendo en la toma de decisiones de Argentina, siendo que en contraposición, se establece que la Junta Militar argentina diseñó la acción militar, destacándose el asombro de los británicos (Bartolomé, 1997). No obstante, la existencia de dos eventos previos al conflicto demuestran que la reacción sorpresiva británica es difícil de argumentar. El incidente de las Islas Thules del Sur consiste en el hecho de que el Reino Unido detectó la presencia argentina en la isla, sin embargo, lo ocultó hasta 1978 reaccionando con una operación de disuasión encubierta: la Operación Journeyman. Esta fue lanzada en 1977 y se basó en el envío de una flota al Atlántico Sur (Lorton, 2011) en medio de la preocupación por una posible actitud beligerante de Argentina, que se mantuvo en secreto por las posibles implicancias legales. Mientras el Informe Franks (1985) sostiene que Argentina nunca supo del despliegue británico, autores como Lorton (2011) afirman lo contrario, señalando que sí se les permitió conocer la presencia naval, lo que habría motivado el retiro argentino. Esta ambigüedad pone en duda si el accionar británico realmente funcionó como estrategia disuasiva o no.

El segundo incidente ocurrió en las Islas Georgias del Sur, cuando el empresario argentino Constantino Davidoff viajó con apoyo de la Armada a desguazar estaciones balleneras, coincidiendo con la planificación de la "Operación Azul" y "Alfa" de la Junta Militar (Franks, 1985). En base al Informe Rattenbach, el gobierno argentino interpretó que el Reino Unido intentaba reforzar su presencia militar y evitar cualquier discusión sobre la soberanía de las islas (1985, párr. 236). El aumento de las tensiones se acrecentó cuando los británicos expresaron públicamente su intención de proteger el territorio con fuerzas navales, siendo un punto de inflexión el envío del HMS Endurance para desalojar a obreros argentinos, ya que se preveía una posible confrontación (Lorton, 2011). Si bien se sostuvo que EE.UU no poseía información sobre los planes argentinos, diversas fuentes revelaron que la NSA (National Security Agency) había detectado movimientos desde días antes y alertado a los británicos, contradiciendo la versión oficial del Foreign Office (Arrosio, 2022). Estas incoherencias fortalecen la hipótesis de que existió una operación de engaño estratégico entre Reino Unido y EE.UU, dado que conocían los preparativos argentinos antes del desembarco del 2 de abril. A pesar de haber existido antecedentes que demostraran la posibilidad de conflicto con Argentina, el SIPRI (Stockholm International Peace Research Institute) demuestra que en los años 1976 y 1981, Londres colaboró con el fortalecimiento militar argentino. Para el año 1976, el Reino Unido realizó una serie de transferencias de armas a Argentina en un valor de 305 millones de SIPRI TIV . Mientras que en 1981, un año previo a la guerra, fue de un valor de 309 millones de SIPRI TIV. Se entregaron destructores, misiles y motores de aeronaves. Asimismo, un documento oficial británico expresó la intención de desplegar fuerzas navales en zonas del Atlántico Sur, junto a Estados Unidos un año previó a la guerra (United Kingdom Government, 1981, párr 32, 34). Esto pone en duda la narrativa británica de haber sido sorprendida por la decisión argentina en 1982, debido a que inmediatamente al inicio del conflicto bélico, el Reino Unido comenzó a interferir en su defensa nacional por medio de un embargo de armas. Esta fue una de las formas más viables para garantizar que el país no se desarrolle militarmente, potenciando la militarización de las Islas Malvinas.

"Política de control de exportaciones estratégica británica a Argentina"

La estrategia que implementó el Reino Unido durante el conflicto del Atlántico Sur fue un embargo de armamento, que: "(...) consistió en bloquear las instituciones y los sectores económicos de los que depende el desarrollo tecnológico militar argentino" (Blinder, 2021, p. 101). Esta sanción fue impuesta por el Reino Unido en conjunto con la Comunidad Económica Europea (CEE), aplicadas en virtud del artículo 113 pero justificadas mediante el artículo 224 del Tratado de Roma (1957) a partir del 16 de abril de 1982 (Vieira, 2016). Dicha sanción comprendió tres etapas. En la primera, se observó un firme respaldo europeo al Reino Unido ante la prohibición generalizada de importaciones, que causaría un cambio de actitud en la Junta Militar, hecho que no ocurrió. Aunque la economía argentina logró resistir inicialmente, las sanciones produjeron efectos significativos a mediano plazo (Ludlow, 2021). En una segunda fase, el consenso europeo se debilitó ante la ausencia de beneficios visibles y la creciente disconformidad de algunos Estados miembros, como Italia o Dinamarca. Además, el hundimiento del Crucero General Belgrano fue clave para que Irlanda también se distanciara debido al hecho similar que representó el hundimiento del Sharelga. Esto generó "una ola de horror y repugnancia" (Irish Report, 1982, p. 3), visto como "una importante victoria militar que, sin embargo, se convirtió en una derrota política" (Edwards, 1984, p. 308). En la última etapa, los países europeos exigieron al Reino Unido reciprocidad en cuestiones internas de la CEE, evidenciando que la cooperación no respondía únicamente a una causa común, sino era un "quid pro quo" de intereses. Finalmente, la sanción multilateral no funcionó, debido a que los Estados participantes no se beneficiaron de la guerra, de modo que la CEE levantó las sanciones el 21 de junio, mientras que los británicos no procedieron con esta decisión, transformando la sanción en unilateral. El Reino Unido no evitó que Europa le vendiera armas a Argentina, ya que implicaba grandes pérdidas para estos en el mercado internacional de armas, por lo que modificó su estrategia. Es decir, comenzó a denegar u otorgar licencias de exportación, por medio de la aplicación de una política de control de exportaciones estratégicas.

La política de control actúa mediante la Orden de Control de Exportaciones (2008), la cual entró en vigencia en 2009, abarcando controles británicos sobre la exportación de artículos militares y paramilitares, controles nacionales de doble uso y controles sobre el comercio (House of Commons, 2010). A partir de esta legislación, se agrega: la "Lista consolidada de artículos militares estratégicos y de doble uso que requieren autorización de exportación. Esta clasifica dos tipos de artículos: aquellos bienes militares que incluyen bienes, software y tecnología que están diseñados o modificados para uso militar; y 2) los bienes de doble uso que engloba a los artículos que están disponibles para comprar comercialmente y normalmente están "listos para usar" pero tienen capacidades mejoradas que son útiles en armas químicas, biológicas, radiológicas, nucleares o convencionales" (Export Control Joint Unit, 2022). La Orden N° 3231 establece en el Anexo IV a Argentina como un país sujeto a los controles más estrictos de las exportaciones y comercio, específicamente en lo relacionado a las mercancías militares, mediante el otorgamiento o denegamiento de licencias de exportación OIEL (licencias de exportación individuales abiertas) o SIEL (licencias de exportación individuales estándar) y el uso de un sistema conocido como SPIRE, por el que se solicitan tales licencias de exportación (United Kingdom, 2021). El gobierno británico sostiene abiertamente que "desde el 3 de abril de 1982, el Reino Unido ha mantenido un embargo nacional de armas contra Argentina" (Hansard, 17 de Diciembre, vol. 322) y su última revisión proviene de 2019. La declaración oficial del Ministerio de Defensa del Reino Unido afirma que su política ha sido no otorgar una licencia de exportación para ningún producto y tecnología militar o de doble uso que se suministre a usuarios finales militares en Argentina, excepto en circunstancias excepcionales. Su posición será continuar rechazando licencias para la exportación y el comercio de bienes que se considere que mejoran la capacidad militar argentina (Export Control Joint Unit, 2019). Es preciso señalar que la sanción se ha mantenido dinámica, dado que ha cambiado en base a los intereses británicos en la región. En estas cuatro décadas, los controles de exportación no

han cesado, por lo que existe la posibilidad de establecer una vinculación entre la política de control de exportaciones estratégicas hacia Argentina con la geopolítica del Atlántico Sur.

"Remilitarización del Atlántico Sur (1982-2022): impacto sobre la defensa argentina"

Una vez finalizada la guerra, comenzó un proceso de militarización en el Atlántico Sur. La presencia militar británica en las islas estuvo acompañada de su mayor aliado, EE.UU, debido a que ambos países entendían que las Islas Malvinas podrían funcionar como una plataforma para el control del Atlántico Sur (Bartolome, 1997). A partir de un análisis de las políticas de defensa de Argentina y del Reino Unido y la política de control de exportaciones, se evidenció los máximos puntos de tensión entre ambos actores.

Entre 1982-1990, se instauró la base militar en Mount Pleasant, concentrando medios y equipo militar, con un aumento del 3% en el gasto británico para el período (Groove, 2002). Se adicionaron fuerzas británicas con fines ofensivos y se concretó el proyecto Zeus (1983), construyendo un radar con alcance suficiente para observar América Latina, Antártida y Atlántico Sur (Parliament UK, 1983). En contraste, Argentina disminuyó abruptamente sus gastos en defensa con la Ley de Defensa Nacional Nº 23.554 (Eissa y Ariella, 2021). Se observa que desde 1982 a 1984, los gastos varían de 2.7 % a 2.2 % del PBI, luego existe una tendencia constante en esos valores, y hacía 1990 disminuyó a 1.5%. Aunado a esto, se inició el embargo de armas, resultando ser favorable en función de la concreción de proyectos británicos, cómo lo fue la construcción de la "Fortaleza Malvinas".

Durante la década 1990-2000, los costos de la base británica decrecieron, concentrándose en su mantenimiento militar. La política restrictiva se sostuvo, denegando licencias de exportaciones estratégicas (House of Commons, 2007). Los gastos argentinos en defensa oscilaron entre 1.5 % y 1.4% del PBI hasta 1995, luego decreció a 1%. En los años 1997 y 1999, las licencias que se solicitaron fueron de uso militar y han sido rechazadas. Más allá de que Argentina se haya adherido como miembro extra OTAN, los británicos no modificaron su política restrictiva. No obstante, entre 2000-2010, los gastos británicos aumentaron, hasta tal punto de superar la capacidad militar de países latinoamericanos. Se registra que en 2003 ingresaron navíos con arsenal nuclear a Malvinas, mientras que en 2007 se realizó la primera exhibición bélica en 25 años (Testa, 2015). Argentina alcanzó su pico presupuestario en 2001 con el 1.2 % del PBI, decreciendo entre 2002-2008, con leve crecimiento al 1% del PBI en 2010. No obstante, la política de control se intensificó en respuesta al aumento del presupuesto argentino.

Entre 2010-2022, se reforzó la modernización de Mount Pleasant, incluyendo cazas Typhoon, helicópteros, fragatas, submarinos nucleares y defensa antiaérea, con inversiones millonarias y sin recortes presupuestarios. Para el año 2015, se emitió un programa de mejoras por 180 millones de libras para un plazo de diez años. En cuanto a los años posteriores, no se ha publicado detalladamente los gastos o costos de las Islas Malvinas para el Reino Unido. No obstante, en el período 2020-2021, se adoptó el concepto operativo integrado, reforzando la coordinación con la US Navy para ampliar el valor estratégico de las Malvinas. Argentina tuvo dos picos leves en gastos de defensa en 2013 y 2017 de 0.9 % del PBI, mientras entre 2018-2022 decayó al 0.4%, observándose que los gastos han sido menores a la década anterior. Por su parte, la política británica se mantuvo restrictiva y activa, rechazando o revocando la mayoría de las licencias de exportación.

Es importante señalar que Argentina ha avanzado en proyectos como la creación del Fondo Nacional de la Defensa (FONDEF) mediante la ley Nº 27.565, pero este presenta sus limitaciones. Este proyecto se propone asignar un financiamiento específico para modernizar, recuperar e incorporar material material (MINDEF, 2023). No obstante, es preciso realizar dos aclaraciones: 1.

El fondo obtiene recursos de los ingresos corrientes para ese año en particular, establecidos por la Ley de Presupuesto; 2. Los recursos del fondo son anunciados en pesos, de modo que el monto "inicial" del FONDEF decrece a medida que la moneda argentina se deprecia en relación al dólar, por lo que no se contempla las adquisiciones provenientes del exterior como objetivo principal (Magnani 2023), demostrando que tal instrumento no aplaca los efectos de la política británica.

La política de control ha ocasionado efectos negativos sobre el sistema de defensa nacional argentino, siendo la Fuerza Aérea y la Armada argentina las más afectadas, lo cual se explica en que el FONDEF ha aportado a la recuperación y modernización perteneciente a estas dos fuerzas. Si bien existe la posibilidad de replantearse la idea de adquirir sistemas de armas de origen chino, los costos de estos serían muy elevados debido a que Argentina siempre ha adquirido sistemas de armas occidentales, siendo que la instrucción de uso sería totalmente nueva (Coman, comunicación personal, octubre 2023). Al momento, resulta complicado para el país adquirir componentes de sistemas de armas extranjeros o modernizar los propios, evitando negociar la tecnología disponible con el Reino Unido. La última publicación del libro Blanco de la defensa ha expuesto que existe un: "(...) impacto negativo que genera en nuestro país la vigencia del embargo de armas impuesto por el Reino Unido tras finalizar el conflicto bélico de 1982, cuyos efectos han sido permanentes" (MINDEF, 2023, p. 24).

Al igual que Argentina, Turquía sufrió un embargo de armas por parte de EE.UU tras la "Operación Chipre", siendo un duro golpe para la Fuerza Aérea turca, dependiente de suministros estadounidenses (Durmaz, 2014; Mevlutoglu, 2017). Esto inició un proceso de crecimiento que, tras cincuenta años, le permitió alcanzar autonomía estratégica en defensa, convirtiéndose en productor de tecnologías militares avanzadas como drones, blindados y sistemas de guerra electrónica (Akgönül et al., 2023). Mediante una política que combinó producción local, importaciones bajo licencia y desarrollo nacional (Bağcı y Kurç, 2016; Mevlutoglu, 2017), y consenso entre oficialismo y oposición del gobierno en torno a la defensa (Seren, 2021), Turquía logró consolidar su industria, fortalecer sus capacidades militares y posicionarse como un actor destacado en el mercado internacional de armas, ocupando el segundo lugar en el ranking de proveedores emergentes (SIPRI) (Akgönül et al., 2023). Es así que la cuestión turca podría constituir un punto de partida para arribar a una solución en la problemática militar argentina.

Reflexiones finales

Las Islas Malvinas poseen una capacidad logística que permite proyectarse al continente antártico, siendo una puerta de entrada estratégica a la región. Argentina cuenta con las condiciones para desarrollarse como pívot en el Atlántico Sur, sin embargo, aún no ha demostrado aspiraciones de convertirse en un actor naval relevante, lo cual se refleja según Marini, en la "falta de conciencia geográfica del Estado". Esta carencia fue aprovechada por el Reino Unido, que implementó una política de control de exportaciones con un marco normativo estricto, manteniendo a Argentina en la "Lista consolidada de artículos militares estratégicos y de doble uso" desde 1982.

Ciertamente, la estrategia británica ha tenido éxito a largo plazo, limitando la capacidad militar argentina por cuatro décadas hasta la actualidad, y consolidando su presencia estratégica en las Islas del Atlántico Sur. El análisis de gastos y equipamiento británico evidencia un carácter ofensivo y un exceso de fuerzas más allá de lo necesario, siendo un propósito estratégico más que defensivo. En contraste, Turquía supo transformar un embargo de armas en un impulso para fortalecer su defensa nacional, desarrollando tecnologías militares avanzadas y proyectando su política de defensa en distintos ámbitos de la sociedad y la política internacional.

Es preciso que Argentina considere la experiencia turca, teniendo en cuenta la realidad geopolítica, de cara a construir una proyección estratégica para América Latina, capaz de anticipar posibles escenarios de conflicto, incluso aquellos que hoy parecen impensados.

REFERENCIAS BIBLIOGRÁFICAS

-AKGÖNÜL et al (2023). Neoclassical Realist Perspective on Militarization of Turkish Foreign Policy. En: Eslami, M., Guedes Vieira, A.V. (eds) The Arms Race in the Middle East. Contributions to International Relations. Springer, Cham. https://doi.org/10.1007/978-3-031-32432-1_9
-ARROSIO, H. A (2022). La comunidad de Inteligencia Británica y el Conflicto del Atlántico Sur. Revista Defensa Nacional N°7. Universidad de la Defensa Nacional. Buenos Aires, Argentina
-BAGCI, H., KURÇ, Ç. (2017). Turkey's strategic choice: buy or make weapons?. Defence Studies, 17(1), 38-62. https://doi.org/10.1080/14702436.2016.1262742
-BARTOLOMÉ, M. C.(1997). El conflicto del Atlántico Sur: la hipótesis de una guerra fabricada. Boletín del Centro Naval, 786, 311-334.
-BLINDER, D. (2021). Falklands/Malvinas' Air Warfare and Its Consequences: A Critical Geopolitical Approach. The Falklands/Malvinas War in the South Atlantic, 85-115.
-EDWARDS, G (1983) Europe and The Falklands Islands Crisis 1982. J. Common Mkt. Semental. , 22 , 295.
-EISSA, S., Ferro Ariella, P. (2018). La política de defensa argentina desde el retorno de la democracia. Una mirada presupuestaria. Defensa Nacional, pp. 99-148. Centro Educativo de las Fuerzas Armadas. CEFA. Argentina.
-EMBASSY OF IRELAND, (1982) "The Falklands Crisis and anglo irish relations" ["La crisis de Malvinas y las relaciones anglo irlandesas"]. Diplomatic Report 168/82 (22 June 1982) Dublin, Republic of Ireland.
-EXPORT CONTROL ACT, 2002. United Kingdom.
-EXPORT CONTROL ORDER, 2008. No. 3231. United Kingdom.
-EXPORT CONTROL JOINT UNIT, DEPARTMENT FOR INTERNATIONAL TRADE DEPARTMENT FOR BUSINESS AND TRADE, (2022) Guidance "UK strategic export controls" [Guía "Controles estratégicos de exportación de Reino Unido"] Last update: 21 November 2023. United Kingdom Government.
-EXPORT CONTROL JOINT UNIT, DEPARTMENT FOR INTERNATIONAL TRADE, DEPARTMENT FOR BUSINESS AND TRADE, (2019) Guidance "Export Licensing policy for Argentina". [Guía "Política de licencias de exportación para Argentina"] United Kingdom Government.
-FRANKS, O. B. (1985). El servicio secreto británico y la Guerra de las Malvinas. Ediciones del Mar Dulce.
-GROOVE, E. (2002). The Falklands War and British Defense Policy. Defense & Security Analysis, 18(4), 307-317. https://doi.org/10.1080/1475179022000024448
-HANSARD, HC Debated Vol. 26, Col. 74 (22 June 1982)
-HOUSE OF COMMONS, 2007 "Strategic Export Controls: 2007 Review". [Control de exportaciones estratégicas: Revisión 2007] HC 117. United Kingdom
-LORTON, R. (2011) Falklands Wars-the History of the Falkland Islands: with particular regard. Paper 11, 1972-1982.
-LUDLOW, N. P. (2021). Solidarity, sanctions and misunderstanding: The European dimension of the Falklands Crisis. The International History Review, 43(3), 508-524. https://doi.org/10.1080/07075332.2020.1791226
-MAGNANI, E. (2023). ¿La defensa nacional como instrumento de desarrollo económico?: El Fondo Nacional para la Defensa (FONDEF) de Argentina. Cuadernos de Política Exterior Argentina. Centro de Estudios en Relaciones Internacionales de Rosario. Universidad Nacional de Rosario, Argentina.
-MARINI, J. F (1980). Conocimiento geopolítico. Revista del Instituto de Derecho Político y Constitucional. Facultad de Derecho. Universidad de Buenos Aires, Argentina.
-MARTIN, L. L. (1992). Institutions and cooperation: Sanctions during the Falkland Islands conflict. International Security, 16(4), 143-178. https://doi.org/10.2307/2539190
-MEVLUTOGLU, A. (2017). Commentary on Assessing the Turkish defense industry: structural issues and major challenges. Defence Studies, 17(3), 282-294.
-MINISTERIO DE DEFENSA ARGENTINA (MINDEF), (2023). FONDEF, Una Política de Estado 2023. Compilación de Agustín Rossi. - 1a ed. - Ciudad Autónoma de Buenos Aires : Universidad de la Defensa Nacional. Argentina.
-NOGUEIRA, C. A. (2022). Malvinas y la competencia por la conectividad en el Atlántico Sur. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, Ciudad Autónoma de Buenos Aires, Argentina
-PARLIAMENT UK, HC Debated Vol 38 C234W. 3 March 1983.

-RATTENBACH, B. (1982). Informe final de la Comisión de Análisis y Evaluación de responsabilidades en el conflicto en el Atlántic
o Sur (Informe Rattenbach). Buenos Aires: Dirección Nacional del Registro Nacional.
-SEREN, M. (2021). Politics, Industry and Academia: Examining Dynamics of Turkish Defense Industry 's Great Leap Forward in the Post-2002 Era. Bilig, (96 (TBMM'NİN 100. YILI ÖZEL SAYISI)), 93-119.
-TESTA, A. (2015). La guerra de Malvinas 02 Abr/14 Jun 1982–Argentina y RUGB y la importancia geoestratégica del archipiélago en el Atlántico Sur. Trabajo Final Integrador. Escuela Superior de Guerra Tte Grl Luis María Campos: Ciudad Autónoma de Buenos Aires. Argentina.
-UNITED KINGDOM GOVERNMENT, (1981): "The United Kingdom Defence Programme: The Way Forward" "El programa de defensa del Reino Unido: El camino a seguir". United Kingdom.
-VIEIRA, R F (2015). O papel dos atores externos no conflito das Malvinas. CLACSO. Buenos Aires, Argentina.

» Infraestructuras críticas marítimas militares

Por TN Lic. Bernardo Collado[3]

Las infraestructuras críticas marítimas militares constituyen un eje estratégico para la proyección de poder naval, el sostenimiento logístico y la interoperabilidad en operaciones conjuntas. Sin embargo, su creciente digitalización y dependencia de sistemas interconectados ha incrementado las vulnerabilidades frente a ciberataques, sabotajes físicos y amenazas híbridas. A partir de ejemplos recientes, como el ciberataque al grupo Maersk en 2017 o los daños a puertos y astilleros en Ucrania durante la guerra actual, el artículo examina los principales riesgos que enfrentan estas infraestructuras y propone un enfoque integral de protección. Se plantean líneas de acción doctrinarias, tecnológicas y político-estratégicas, con énfasis en resiliencia, cooperación civil-militar e innovación. El objetivo es repensar la defensa naval más allá de los buques, incorporando la seguridad de las infraestructuras como parte central de la estrategia marítima contemporánea.

Visualización conceptual sobre la seguridad en las infraestructuras críticas marítimas militares.

Fuente: Imagen generada digitalmente por IA.

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

INTRODUCCIÓN.

La historia naval demuestra que la fortaleza de una armada nunca ha dependido únicamente de sus buques de guerra. Desde los arsenales imperiales hasta las modernas bases navales interconectadas, las infraestructuras críticas han sido el verdadero pilar que sostiene la capacidad operativa.

En el presente siglo, la digitalización, la automatización portuaria y la creciente interdependencia global han transformado esos espacios en nodos vulnerables, expuestos a actores estatales y no estatales capaces de proyectar ataques tanto físicos como cibernéticos.

Los casos recientes lo evidencian con claridad: el ciberataque de 2017 contra el grupo Maersk paralizó temporalmente operaciones portuarias en todo el mundo; la guerra en Ucrania mostró cómo los astilleros y puertos militares se convierten en objetivos prioritarios de ataques de misiles, drones y sabotajes híbridos; e incidentes de intrusión en redes navales de la OTAN alertan sobre la fragilidad de la dimensión digital de las fuerzas marítimas.

Este panorama plantea un interrogante central: ¿cómo proteger estas infraestructuras sin las cuales la fuerza naval, por más avanzada que sea, se convierte en un cascarón vacío? Para responder, es necesario un enfoque integral que combine medidas técnicas de ciberdefensa, estrategias de redundancia y resiliencia, doctrina militar actualizada y marcos de cooperación internacional.

El análisis que sigue busca contribuir a este debate, proponiendo un marco de reflexión y acción que permita fortalecer la seguridad de las infraestructuras críticas marítimas militares frente a un escenario global caracterizado por la incertidumbre, la complejidad y la amenaza híbrida.

INFRAESTRUCTURAS CRÍTICAS EN EL ÁMBITO MARÍTIMO-MILITAR.

Concepto y marco general:

Las infraestructuras críticas son aquellas instalaciones, sistemas, servicios o recursos cuya perturbación o destrucción tendría un impacto grave sobre la seguridad nacional, la economía o el bienestar de la población. La Unión Europea, por ejemplo, las define como "aquellas cuya interrupción afectaría de manera significativa el funcionamiento de la sociedad y el Estado" (Consejo de la UE, 2008). En Estados Unidos, el Departamento de Seguridad Nacional establece un criterio similar, destacando que su afectación compromete funciones esenciales de gobierno, defensa y vida cotidiana (DHS, 2013).

En este marco, resulta necesario distinguir entre infraestructura crítica civil y militar. La primera incluye sectores como energía, transporte, agua, comunicaciones o finanzas, que sostienen el funcionamiento general del país. La segunda, vinculada al ámbito militar, comprende aquellas instalaciones y sistemas indispensables para garantizar la defensa y la proyección de poder. En el entorno naval, esto implica desde puertos de guerra, arsenales y astilleros hasta los sistemas de mando y control, redes de comunicaciones y plataformas logísticas que hacen posible la operatividad de las fuerzas en el mar.

La creciente interdependencia entre infraestructura civil y militar es hoy un factor central. Muchos sistemas navales dependen de proveedores civiles, de redes energéticas nacionales o de servicios de conectividad global. Este entrelazamiento multiplica las vulnerabilidades: un ataque a una red civil de energía o telecomunicaciones puede repercutir de inmediato sobre la capacidad operativa de una fuerza naval.

Por ello, el concepto de infraestructura crítica debe entenderse como un sistema integrado, en el que la protección de lo civil y lo militar se entrelaza de manera inseparable.

Identificación y clasificación:

En el espacio marítimo-militar, las infraestructuras críticas se agrupan en distintos niveles según su función y su grado de vulnerabilidad. Entre las más relevantes, se destacan:

1. Puertos militares y arsenales navales:
   1.1. Constituyen la base de operaciones y sostenimiento de las flotas. Su afectación puede dejar inoperantes a unidades navales enteras.
   1.2. Ejemplo: el ataque con drones a la base naval de Sebastopol en 2022, que puso en evidencia la vulnerabilidad de puertos militares ante medios asimétricos.
2. Astilleros y centros de mantenimiento:
   2.1. Aseguran la capacidad de reparación, modernización y extensión de vida útil de buques y submarinos.
   2.2. Ejemplo: durante la Segunda Guerra Mundial, los astilleros estadounidenses fueron objetivos prioritarios para sabotajes e inteligencia enemiga, dado que constituían un "cuello de botella" estratégico.
3. Redes de mando, control y comunicaciones (C2/C4ISR):
   3.1. Integran sistemas de vigilancia, enlace táctico, sensores y comunicaciones satelitales. Son esenciales para garantizar conciencia situacional y capacidad de respuesta.
   3.2. Ejemplo: en 2007, Estonia sufrió un ataque cibernético a gran escala que, aunque dirigido contra infraestructura civil, mostró cómo una ofensiva digital puede paralizar también sistemas militares interconectados.
4. Infraestructura energética asociada al poder naval:
   4.1. Incluye depósitos de combustible, plantas de generación eléctrica y líneas de abastecimiento.
   4.2. Ejemplo: en el conflicto del Golfo de 1991, el ataque aliado a la infraestructura petrolera de Kuwait y de Irak limitó severamente la capacidad de sostener operaciones prolongadas.
5. Infraestructura logística y de transporte estratégico:
   5.1. Aeropuertos militares costeros, depósitos, oleoductos y rutas de transporte que permiten la movilización y el reabastecimiento de fuerzas.
   5.2. Ejemplo: durante la guerra de las Malvinas, la dependencia de puntos logísticos limitados en el Atlántico Sur evidenció la vulnerabilidad de las líneas de sostenimiento.
6. Cables submarinos y redes digitales:
   6.1. Aunque civiles en origen, son vitales para las operaciones navales modernas al sostener el flujo de datos global.
   6.2. Ejemplo: el sabotaje a los gasoductos Nord Stream en 2022 reavivó el debate sobre la seguridad de las infraestructuras submarinas, entre ellas cables de fibra óptica que también pueden ser blanco militar.

PRINCIPALES AMENAZAS Y RIESGOS CONTEMPORÁNEOS.

La protección de infraestructuras críticas en el ámbito marítimo-militar exige comprender un espectro de amenazas que combina medios tradicionales con herramientas propias de la guerra híbrida y la innovación tecnológica.

1. Ataques convencionales de precisión:
   1.1. Los misiles de crucero, drones de ataque y municiones guiadas permiten golpear objetivos portuarios, arsenales o depósitos energéticos con alta eficacia.

1.2. Ejemplo: en 2017, un ataque con misiles balísticos hutíes impactó cerca de la base naval saudí en Yedá, evidenciando cómo fuerzas no estatales pueden emplear armamento de precisión.

2. Terrorismo y sabotaje interno:
   2.1. Los grupos terroristas pueden atentar contra puertos, astilleros o depósitos de combustible, generando daños estratégicos a bajo costo.
   2.2. Ejemplo: el ataque terrorista al USS Cole en 2000, mientras estaba atracado en Adén, reveló la vulnerabilidad de las unidades en puerto frente a pequeños equipos con alta capacidad destructiva.

Atentado en Yemen al USS Cole que dejó a 17 marinos muertos. Fuente: https://www.nytimes.com/article/uss-cole-bombing-trial.html.

3. Ciberataques y guerra informacional:
   3.1. Los sistemas de mando, control y comunicaciones (C2/C4ISR) dependen de redes digitales, expuestas a intrusiones, malware o denegación de servicios.
   3.2. Ejemplo: en 2021, el puerto de Houston resistió un ataque cibernético atribuido a un grupo extranjero que buscaba comprometer sistemas de acceso y vigilancia.
4. Drones y vehículos no tripulados:
   4.1. Los UAV (Unmanned Aerial Vehicles) y USV (Unmanned Surface Vehicles) se consolidan como medios asimétricos capaces de atacar infraestructuras a bajo costo.
   4.2. Ejemplo: el ataque con drones navales ucranianos contra Sebastopol en 2022 mostró la efectividad de esta táctica para saturar defensas portuarias.
5. Amenazas híbridas y desinformación:
   5.1. La manipulación informativa y la guerra cognitiva pueden paralizar la respuesta militar, generar pánico social o desviar recursos, debilitando la protección de instalaciones críticas.
   5.2. Ejemplo: campañas de desinformación en el Mar Negro han buscado erosionar la confianza en la seguridad marítima, afectando decisiones estratégicas.
6. Sabotaje a infraestructuras energéticas y submarinas:
   6.1. Los gasoductos y cables submarinos son objetivos de difícil vigilancia pero de altísimo impacto geopolítico.
   6.2. Ejemplo: la explosión de los gasoductos Nord Stream (2022) mostró que actores estatales o paraestatales pueden alterar el equilibrio energético y militar de una región mediante ataques encubiertos.

ESTRATEGIAS DE PROTECCIÓN Y RESILIENCIA.

La protección de infraestructuras críticas marítimas militares no puede limitarse a medidas aisladas de seguridad. Requiere un enfoque integral que combine doctrina, tecnología, gestión del riesgo y cooperación.

En primer lugar, resulta esencial incorporar la ciberseguridad al marco normativo y doctrinario de las instituciones navales, siguiendo las recomendaciones de organismos como la Organización Marítima Internacional (IMO) y las guías de la industria (BIMCO, 2021).

La alineación con estándares como el NIST Cybersecurity Framework permite establecer responsabilidades claras y asegurar procesos de mejora continua que contemplen tanto la tecnología de la información (IT) como la tecnología operacional (OT).

Desde el punto de vista técnico, la defensa debe basarse en el principio de defensa en profundidad. Esto implica segmentar las redes críticas, limitar privilegios de acceso, monitorear anomalías y desplegar sistemas de detección que permitan identificar ataques en fases tempranas. La evidencia de incidentes previos muestra que las intrusiones en sistemas como AIS, ECDIS o VSAT suelen detectarse tarde, cuando el daño ya está consolidado. Por ello, es fundamental contar con sensores que registren comportamientos anómalos y con equipos capaces de responder de manera inmediata.

Otra dimensión clave es la cadena de suministro. Astilleros, proveedores de software, sistemas de comunicaciones satelitales y empresas de mantenimiento forman parte de la red que sostiene la operatividad naval.

Sin embargo, muchas veces no existen requisitos uniformes de seguridad ni mecanismos de auditoría. Incorporar cláusulas contractuales que obliguen a los proveedores a garantizar transparencia, tiempos de respuesta ante vulnerabilidades y planes de contingencia es un paso imprescindible para reducir la exposición.

La resiliencia operativa se apoya, además, en la capacidad de continuar funcionando en escenarios de degradación. El ataque de ransomware a Maersk en 2017 demostró cómo la ausencia de planes de continuidad puede paralizar por completo operaciones portuarias y logísticas.

En el ámbito militar, esto se traduce en la necesidad de mantener procedimientos alternativos, entrenar al personal en la ejecución de operaciones manuales y probar regularmente la capacidad de sostener funciones esenciales sin depender de la red principal.

La dimensión humana es igualmente crítica. La formación del personal en conciencia cibernética, disciplina en el uso de dispositivos externos y conocimiento de protocolos de emergencia reduce significativamente la superficie de ataque. Asimismo, deben existir roles bien definidos, como responsables de ciberseguridad naval, enlaces con agencias civiles y custodios de activos críticos, que garanticen la coordinación de respuestas.

Finalmente, la ciberdefensa debe asumirse como parte del planeamiento operacional. El ciberespacio ya no es solo un apoyo, sino un dominio en el que se combate directamente. La doctrina internacional ha avanzado en este sentido, reconociendo la necesidad de mantener la capacidad de "luchar a través de la perturbación" (fight through). Para ello, es indispensable sincronizar la protección de infraestructuras críticas con sistemas C4ISR, ejercicios de mesa y simulaciones realistas que pongan a prueba la preparación de las fuerzas.

Las estrategias de protección y resiliencia requieren una aproximación escalonada y multidimensional: gestión del riesgo, arquitectura técnica, seguridad de la cadena de suministro, continuidad operativa, cultura organizacional y doctrina integrada. Solo a través de este enfoque sistémico es posible garantizar que las infraestructuras críticas marítimas militares puedan resistir, recuperarse y adaptarse frente a un entorno cada vez más complejo y hostil.

CASOS Y LECCIONES APRENDIDAS.

La teoría sobre infraestructuras críticas marítimas militares encuentra su mayor fuerza cuando se confronta con la evidencia empírica. Los incidentes recientes han demostrado que tanto actores estatales como no estatales pueden afectar con relativa facilidad estos sistemas, generando consecuencias estratégicas desproporcionadas en relación con los medios empleados.

El caso más citado es el ataque de ransomware NotPetya en 2017 contra el grupo Maersk. Aunque su objetivo inicial no fue militar, el impacto global paralizó terminales portuarias, afectó operaciones logísticas y obligó a reinstalar miles de servidores y estaciones de trabajo. La lección para el ámbito naval es clara: una dependencia excesiva de sistemas digitales interconectados sin redundancias adecuadas puede inmovilizar no solo al comercio, sino también a la movilidad estratégica militar que depende de esos mismos puertos.

Otro ejemplo contundente es el de la guerra en Ucrania. Desde 2022, los puertos y astilleros militares se han convertido en blancos constantes de ataques con misiles, drones y sabotajes. La base naval de Sebastopol sufrió múltiples incursiones con vehículos no tripulados de superficie, que consiguieron penetrar las defensas tradicionales. Estos incidentes confirmaron que las amenazas asimétricas, combinadas con tecnologías relativamente accesibles, pueden degradar la operatividad de instalaciones portuarias de alto valor estratégico.

Buque de guerra Tarantul-IIIde la Flota del Mar Negro en el puerto de Sebastopol.

Fuente: https://efe.com/mundo/2023-03-22/ataque-con-drones-sobre-crimea-y-kiev/.

También debe mencionarse el caso de los gasoductos Nord Stream en 2022, cuya destrucción puso de relieve la vulnerabilidad de infraestructuras submarinas críticas. Aunque no se trató de una instalación estrictamente militar, el ataque evidenció que las líneas energéticas y de comunicaciones bajo el mar, incluidos cables de fibra óptica, son objetivos tentadores para operaciones encubiertas y de difícil atribución. Para las fuerzas navales, proteger estas infraestructuras es tan relevante como defender una base o un arsenal.

Incluso incidentes de terrorismo clásico, como el ataque al USS Cole en 2000 en el puerto de Adén, mantienen vigencia como advertencia. Un grupo reducido, con recursos limitados, logró infligir severos daños a un destructor estadounidense en condiciones de aparente seguridad. La lección aquí es que la amenaza no siempre proviene de sofisticados ciberataques o armas de precisión, sino que puede manifestarse a través de tácticas simples pero letales, especialmente durante períodos de atraque o reabastecimiento.

En conjunto, estos casos enseñan que la vulnerabilidad de las infraestructuras críticas marítimas militares no es una hipótesis abstracta, sino una realidad comprobada.

Cada incidente refuerza la necesidad de integrar la ciberdefensa, la protección física y la resiliencia organizacional dentro de un marco coherente de seguridad. Ignorar estas experiencias sería repetir errores en un entorno donde la adaptación rápida es condición de supervivencia estratégica.

CONCLUSIONES.

Las infraestructuras críticas marítimas militares constituyen el núcleo invisible del poder naval. Sin puertos, arsenales, astilleros, centros de mando y redes digitales seguras, ninguna flota puede sostener operaciones prolongadas ni proyectar fuerza más allá de sus aguas jurisdiccionales.

Los casos recientes, desde el ciberataque a Maersk hasta la vulnerabilidad de los puertos ucranianos y la destrucción del Nord Stream, demuestran que estas infraestructuras no solo son objetivos prioritarios, sino también altamente expuestas a un amplio rango de amenazas, desde el sabotaje físico hasta el ciberataque sofisticado. La principal lección es que la defensa de estas instalaciones requiere un enfoque integral: doctrinario, tecnológico, organizacional y político-estratégico.

No basta con reforzar muros o instalar firewalls; se necesita resiliencia, redundancia, cultura de seguridad y cooperación interagencial e internacional. La capacidad de "luchar a través de la perturbación", fight through, se vuelve un principio rector: aún bajo ataque, la infraestructura debe seguir sosteniendo la operatividad naval.

En un mundo interdependiente, donde lo civil y lo militar comparten infraestructuras y vulnerabilidades, el desafío es proteger aquello que constituye la base misma de la disuasión y la defensa marítima. Quien domine o degrade estas infraestructuras controlará, en gran medida, el acceso al mar y la libertad de acción de las fuerzas navales.

¿Podrá una fuerza naval sostener su poder en el mar si sus infraestructuras críticas son neutralizadas antes de que se dispare el primer cañón?

BIBLIOGRAFÍA.

·BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO. (2017). Guidelines on cyber security onboard ships. Version 2.0. Maritime Global Security. https://www.maritimeglobalsecurity.org/media/1014/c-users-jpl-onedrive-bimco-desktop-guidelines_on_cyber_security_onboard_ships_version_2-0_july2017.pdf

·BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO. (2021). Cyber security guidelines. International Chamber of Shipping. https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf

·Boyes, H. (2014). Maritime cyber security – Securing the digital seaways. Engineering & Technology Reference. https://www.researchgate.net/publication/273292020_Maritime_Cyber_Security_-_Securing_the_Digital_Seaways

·Clavijo Mesa, L., Gaitán-Angulo, M., Daza, R., & Jiménez, L. (2025). Maritime cyber security: Concepts, problems and models. Journal of Transportation Security, 18(2), 101–122. https://www.sciencedirect.com/science/article/abs/pii/S1366554525000122

·Cyber-SHIP Lab. (2023). Cyber-SHIP Lab Symposium programme. University of Plymouth. https://wwwcdn.imo.org/localresources/en/MediaCentre/Documents/DPC23452_Cyber-SHIP_Lab_Symposium_programme.pdf

·DHS. (2024). Maritime trade and port cybersecurity. U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/2024-09/2024aepphasellusmaritimetradeandportcybersecurity.pdf

·Fonseca, R. (2014). Infraestructuras críticas y seguridad nacional. Revista ESG, (588), 172–187. Escuela Superior de Guerra.

https://cefadigital.edu.ar/bitstream/1847939/993/1/Revista%20ESG%20no.588-2014_Fonseca_172.pdf
·International Hydrographic Organization. (2023). Maritime cybersecurity primer (UKMDA ILO). https://iho.int/uploads/user/Inter-Regional%20Coordination/RHC/SWPHC/Events/1-Day%20VTC%20Agenda%20Item%202%20-%2020230213-Maritime_cybersecurity_primer_UKMDAILO-0_opt.pdf
·Li, M. (2024). Maritime cybersecurity: A comprehensive review. ResearchGate. https://www.researchgate.net/publication/383549133_Maritime_Cybersecurity_A_Comprehensive_Review/citation/download
·Meland, P. H., Bernsmed, K., Nesheim, D., & Jaatun, M. G. (2021). A retrospective analysis of maritime cyber security incidents. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 15(1), 59–66. https://www.transnav.eu/Article_A_Retrospective_Analysis_of_Maritime_Cyber_Security_Incidents_Meland,59,1144.html
·NATO CCDCOE. (2021). Maritime cyber security: Concepts, problems and models. Academia.edu. https://www.academia.edu/81074218/Maritime_Cyber_Security_concepts_problems_and_models
·Nordal, O., & TalTech Maritime Academy. (2023). Maritime cyber security research. Tallinn University of Technology. https://taltech.ee/en/estonian-maritime-academy/areas-of-advance/maritime-cyber-security#p42533
·Pavur, J., & Martin, L. (2024). Information security challenges in the maritime domain. Information, 15(11), 710. https://www.mdpi.com/2078-2489/15/11/710
·Samaniego, R., & Universidad del Centro de Florida. (2022). Maritime cyber security: An overview. Embry-Riddle Aeronautical University Commons. https://commons.erau.edu/cgi/viewcontent.cgi?article=2377&context=publication
·Seapower Centre Australia. (2021). Soundings No. 42. https://seapower.navy.gov.au/sites/default/files/2023-02/Soundings_No_42.pdf
·Thiele, R. (2018). The impact of cyber threats on naval operations. ISPSW Strategy Series, No. 530. ETH Zürich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/ISPSW-530%20Thiele.pdf
·Torres, M. (2016). Ciberseguridad marítima: retos y oportunidades. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. https://esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-49.pdf
·Zeng, Y., Li, J., & Wu, H. (2024). Maritime cybersecurity: Advances, risks and resilience. arXiv preprint arXiv:2409.11417. https://arxiv.org/pdf/2409.11417
·Observatorio de Tácticas Navales. (2025). Boletín N° 42: Seguridad marítima y ciberdefensa naval. FA-ARA. https://fadara.armada.mil.ar/assets/publicaciones/doc/boletin-420250627103110.pdf

» Cyber Kill Chain

Por TC Lic. Cristian Matías Ledesma[1]

La Cyber Kill Chain, o cadena de ciberataque, representa un modelo de seguridad que describe las distintas etapas que componen un ciberataque. Desarrollado por Lockheed Martin en el año 2011, este marco se fundamenta en un concepto de origen militar, adaptado para la comprensión y modelado de intrusiones dentro de las redes informáticas. Su propósito primordial radica en facilitar la comprensión y la anticipación de las diversas fases que constituyen un ataque cibernético, desde su fase inicial de reconocimiento hasta la culminación en la exfiltración de datos o la consecución del objetivo final del atacante. Al ofrecer una representación visual de estas etapas, las organizaciones pueden planificar de manera más efectiva sus estrategias de defensa y seleccionar las herramientas más apropiadas para mitigar las vulnerabilidades, responder a los ataques en curso y, en última instancia, minimizar los riesgos inherentes al ciberespacio. La presentación secuencial de un proceso inherentemente complejo que ofrece la Cyber Kill Chain permite a los equipos de seguridad anticipar las posibles acciones de los atacantes, fortaleciendo las defensas en cada etapa del ciclo de vida del ataque. Esta perspectiva transforma la Ciberdefensa de una postura meramente reactiva a una estrategia proactiva y fundamentada.

Un precursor notable de la Cyber Kill Chain es la estrategia militar F2T2EA (Find, Fix, Track, Target, Engage, Assess) empleada por la Fuerza Aérea de los Estados Unidos. La transposición de un modelo militar al ámbito de la ciberseguridad subraya la naturaleza intrínsecamente adversarial de este campo, donde las acciones del atacante deben ser consideradas dentro de una estructura estratégica que los defensores pueden analizar y, en última instancia, contrarrestar. La analogía militar del término "kill chain" evoca la idea de una secuencia de eventos necesarios para "eliminar" un objetivo. En el contexto militar, esto implica una serie de pasos coordinados y deliberados. Al aplicar esta mentalidad al campo de la Ciberdefensa, se reconoce que los ciberataques no son incidentes fortuitos, sino procesos estructurados que se desarrollan con objetivos claramente definidos. Esta perspectiva permite a los profesionales de la

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

seguridad abordar la defensa con una mentalidad estratégica similar, buscando activamente interrumpir la "cadena" del atacante en cualquier punto vulnerable a lo largo de su progresión.

A pesar de la constante evolución del panorama de las amenazas cibernéticas, la Cyber Kill Chain ha mantenido su relevancia como una herramienta fundamental para salvaguardar la seguridad de las empresas y organizaciones. En un entorno donde las ciberamenazas han proliferado, abarcando desde el malware y el ransomware hasta los ataques sofisticados orquestados por actores estatales, se hace imprescindible una comprensión exhaustiva de los mecanismos subyacentes a su ejecución y las estrategias para su neutralización. Esto la convierte en una base sólida sobre la cual se pueden desarrollar estrategias de defensa capaces de adaptarse a las amenazas emergentes en el dinámico panorama de la ciberseguridad.

Descripción de las fases

1. Reconocimiento

En esta fase inicial el atacante recopila información sobre el objetivo (organización, red o individuo) para planificar el ataque. Se emplean fuentes abiertas (OSINT)[1] y escaneos activos: búsquedas en web y redes sociales, análisis de dominios y WHOIS, fingerprinting[2] tecnológico y escaneos de puertos para identificar servicios expuestos. Históricamente era un proceso manual; hoy se automatiza con herramientas de scraping e incluso IA, aprovechando datos públicos de empleados y arquitecturas de red. El propósito es descubrir vulnerabilidades explotables sin alertar al objetivo.

2. Armamento (Weaponization)

Aquí el atacante convierte la información recolectada en herramientas de ataque. Se crean o adaptan exploits[3], malware y documentos maliciosos específicos para explotar las vulnerabilidades identificadas. Por ejemplo, puede ensamblar un troyano en un PDF, empaquetar un ransomware modificado para evadir antivirus, o crear un ejecutable personalizado. En esta etapa se enfoca en la personalización: se ajusta el malware al entorno de la víctima (sistema operativo, versiones de software, idioma, etc.) para aumentar su sigilo y efectividad. Las técnicas han evolucionado de código estático a malware polimórfico/obfuscado (a menudo asistido por IA) que cambia constantemente su firma para evadir la detección. Además, hoy los atacantes disponen de servicios de malware-as-a-service (MaaS), compran kits de exploits empaquetados e incluso certificados digitales comprometidos, en lugar de desarrollar todo internamente.

3. Entrega (Delivery)

El atacante envía el arma preparada al entorno de la víctima por el canal más efectivo. Esto puede ser un correo spear-phishing con un adjunto malicioso o enlace a un servidor comprometido, la infectación de un sitio web confiable (watering hole), la inserción de malware en un dispositivo USB/IoT[4] utilizado por la organización, o un ataque a la cadena de suministro (actualización de software comprometida). También se aprovechan hoy plataformas legítimas para camuflar archivos maliciosos. La fase de entrega ha evolucionado con técnicas avanzadas de ingeniería social (mensajes muy realistas, incluso generados con IA) y con el uso de canales legítimos (por ejemplo, enlaces en intranets o servicios cloud) para evadir los controles.

4. Explotación (Exploitation)

Aquí ocurre la "detonación" del ataque: el exploit se activa y el código malicioso se ejecuta, logrando el primer acceso efectivo. Por ejemplo, al abrir un documento Word infectado se vulnera el software Office; o al visitar una web comprometida, el navegador ejecuta un exploit. Se aprovechan vulnerabilidades de software (ya sea conocidas –p. ej. un zero-day– o viejas no parchadas) y técnicas fileless. Hoy en día muchos exploits operan enteramente en memoria usando herramientas legítimas del sistema para evitar la detección. Esta fase es crítica porque es el punto de no retorno: al explotarse una vulnerabilidad, el atacante obtiene una escalada de privilegios. En entornos modernos los atacantes programan cheques de sandbox para que el exploit no se active en entornos de prueba, retrasando la ejecución hasta condiciones reales.

5. Instalación (Installation)

Luego de explotar la vulnerabilidad, el atacante busca establecerse permanentemente. En esta fase se instala malware que mantiene acceso persistente. Por ejemplo, el atacante puede instalar un servicio o driver malicioso, configurar un web shell en un servidor web o utilizar herramientas legítimas para crear persistencia ("living-off-the-land"). También es común crear o habilitar cuentas ocultas (usuarios con privilegios elevados) para acceder repetidamente más tarde. Aunque hoy existen técnicas fileless y basadas en la nube, muchas intrusiones avanzadas aún terminan con módulos maliciosos instalados: backdoors adaptativos que se comunican con C2 cuando se pueda.

6. Comando y Control (Command and Control, C2)

En esta fase el atacante establece un canal de comunicación bidireccional entre la víctima y sus servidores. Esto le permite enviar órdenes al malware y extraer datos robados. Los canales C2 modernos son muy sigilosos: aprovechan protocolos legítimos para mimetizar el tráfico. También se abusa de servicios públicos: por ejemplo, almacenar comandos en repositorios de GitHub, usar hojas de cálculo en Google Sheets o servicios de mensajería como Telegram/Signal. Se implementan mecanismos redundantes para resiliencia. El resultado es que, aunque el atacante ya controle el sistema, las comunicaciones pasan desapercibidas por defensas tradicionales.

7. Acciones sobre el objetivo (Actions on Objectives

Esta es la fase final: el atacante ya controla completamente el entorno comprometido y ejecuta sus objetivos maliciosos. Dependiendo de la motivación (espionaje, sabotaje, fraude, etc.), llevará a cabo actividades como robo de información sensible, extorsión mediante ransomware, movimiento lateral adicional o manipulación de sistemas. Por ejemplo, puede exfiltrar bases de datos de clientes o propiedad intelectual para revenderlas, cifrar archivos críticos exigiendo rescate (a menudo combinando esto con amenazas de filtración), propagar el ataque a socios y proveedores (movimiento lateral), o sabotear infraestructuras (destruir archivos, inducir errores operativos). Grupos APT[5] operan con paciencia extrema: permanecen meses dentro del sistema aprendiendo flujos de trabajo internos y esperando el momento adecuado. En esta fase, el atacante ya no se oculta: su actividad apunta directamente al daño.

El enfoque por fases facilita inspeccionar dónde faltan controles o alertas. Al mapear cada etapa contra las defensas existentes, se descubren puntos ciegos. Por ejemplo, si no hay monitoreo de correlación de logs durante la entrega de malware, es una brecha que la kill chain deja en evidencia. Como señalan expertos, el modelo ayuda a "identificar gaps en sus defensas" y planificar mitigaciones. De esta forma se asegura cobertura de detección en cada paso: por ejemplo, implementar IDS/IPS y honeypots en fases tempranas, y reforzar registros de eventos y segmentación en fases posteriores. Además, la Kill Chain combina bien con otros marcos: se recomienda usarla junto a MITRE ATT&CK. Un buen enfoque es usar la kill chain para ubicar en qué fase está un ataque, e identificar con ATT&CK las técnicas específicas usadas en esa fase. En

la práctica esto se refleja en las reglas de detección del SIEM: se crean alertas basadas en técnicas concretas (p.ej. exploits, TTPs del atacante) y luego se clasifican por fase de la kill chain para priorizar la respuesta. Así, la organización tiene un diagnóstico claro de qué tipo de actividad (por ejemplo phishing, movimientos laterales, exfiltración) puede ocurrir en cada eslabón, y evalúa qué controles adicionales requiere.

Integración con SIEM, EDR, XDR y SOC

La integración del modelo Kill Chain en sistemas de seguridad modernos como SIEM, EDR, XDR y SOC[6] permite una gestión más eficiente y coordinada de las amenazas cibernéticas. En los SIEM, como Microsoft Sentinel, se analizan y correlacionan registros provenientes de la red, correo y endpoints para detectar ataques multietapa, combinando eventos que en conjunto revelan comportamientos anómalos en diferentes fases del ataque. Por ejemplo, al identificar que un escaneo es seguido por un exploit, el SIEM genera una alerta consolidada que refleja la progresión del ataque.

Los sistemas EDR se enfocan en monitorear y responder a actividades maliciosas en los endpoints durante fases críticas como la explotación o instalación de malware, aislando procesos sospechosos. El XDR amplía esta visión integrando telemetría de múltiples fuentes, como usuarios, dispositivos y redes, lo que permite detectar patrones complejos que involucren distintos vectores, y así coordinar respuestas más efectivas.

En los SOC, la Kill Chain estructura los procesos de detección y respuesta, ayudando a los analistas a contextualizar los incidentes y anticipar las próximas acciones del atacante. Esto facilita aplicar controles específicos para cada etapa, como reforzar la inteligencia de amenazas en la fase de reconocimiento, desplegar filtros antiphishing en la fase de entrega o aplicar parches y soluciones EDR en la fase de explotación. Además, este enfoque por fases alimenta la automatización mediante SOAR y playbooks, donde cada etapa tiene respuestas definidas, como bloquear dominios maliciosos durante la fase de comando y control.

La efectividad de este modelo se ha evidenciado en múltiples estudios de caso, desde ataques históricos como WannaCry, el ataque de phishing al Comité Nacional Demócrata o el gusano Stuxnet, hasta incidentes más recientes como el ransomware contra Colonial Pipeline. Estos análisis muestran que la detección y mitigación en fases tempranas, por ejemplo parcheando vulnerabilidades antes de que sean explotadas, puede evitar el desarrollo completo de un ataque. Además, en ejercicios de simulación Red Team/Blue Team se emplea la Kill Chain para recrear tácticas y técnicas de ataque (TTPs), permitiendo a los defensores clasificar eventos según la fase del ataque y optimizar estrategias de detección y respuesta. Este enfoque ha demostrado reducir falsos positivos y acelerar la contención de incidentes, mejorando así la resiliencia de las organizaciones frente a amenazas cibernéticas.

¿Qué impacto tiene comprender este modelo?

Comprender el modelo de ataque por fases tiene un impacto directo y crítico en la capacidad defensiva de cualquier organización que custodie información sensible. Esta comprensión no puede ser superficial ni quedar limitada a unos pocos especialistas: constituye un requisito estratégico.

Cada fase del modelo aporta información clave sobre el ciclo ofensivo del adversario, pero es durante el Reconocimiento donde se define el éxito o el fracaso de lo que sigue. En ese momento, el atacante construye su mapa: identifica estructuras internas, recolecta nombres, herramientas utilizadas, lenguaje institucional y relaciones jerárquicas. Aunque no sea información técnica, resulta fundamental para diseñar campañas dirigidas —especialmente de ingeniería social— capaces de evadir defensas tradicionales.

En este contexto, herramientas como los SIEM (Security Information and Event Management) y los SOC (Security Operations Centers) cumplen un rol decisivo. No alcanza con disponer de estas capacidades: deben integrarse dentro de una estrategia defensiva coherente, con reglas de correlación diseñadas para detectar patrones de Reconocimiento que suelen pasar inadvertidos cuando el enfoque se limita a contener incidentes.

Ninguna tecnología, sin embargo, reemplaza la necesidad de formación. Se requiere una estrategia de capacitación en ciberdefensa amplia, estructurada y sostenida en el tiempo. La ausencia de preparación formal y de doctrina específica genera una dependencia riesgosa de la intuición y la voluntad individual. Frente a adversarios que operan con planificación, recursos y conocimiento del entorno, se necesita algo más que respuesta: es indispensable comprender la amenaza desde su origen.

Negar al adversario la posibilidad de realizar un Reconocimiento efectivo es una forma concreta de degradar su capacidad ofensiva. Impedir el acceso a información contextual lo obliga a improvisar, reduce la efectividad de sus vectores y limita su persistencia. La defensa no comienza cuando se contiene el ataque, sino cuando se impide que el atacante entienda cómo funciona el entorno al que apunta.

Y esa capacidad —en la mayoría de los entornos— no está garantizada.

BIBLIOGRAFIA

Referencias Principales

Lockheed Martin (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.*

Hutchins, E., Cloppert, M., & Amin, R. (2011). "Intelligence-Driven Computer Network Defense." Originally published by Lockheed Martin.

MITRE ATT&CK® Framework. (n.d.). *Tactics and Techniques.* Available at https://attack.mitre.org/

Documentación de MITRE ATT&CK (por fase)

Reconnaissance (TA0043): https://attack.mitre.org/tactics/TA0043/

Initial Access (TA0001): https://attack.mitre.org/tactics/TA0001/

Execution (TA0002): https://attack.mitre.org/tactics/TA0002/

Persistence (TA0003): https://attack.mitre.org/tactics/TA0003/

Privilege Escalation (TA0004): https://attack.mitre.org/tactics/TA0004/

Command and Control (TA0011): https://attack.mitre.org/tactics/TA0011/

Collection (TA0009), Exfiltration (TA0010), Impact (TA0040): https://attack.mitre.org/tactics/

Artículos y Entradas Web

- "What is LockBit Ransomware?" Akamai Glossary.
- "EternalBlue," Wikipedia. https://es.wikipedia.org/wiki/EternalBlue
- "Office of Personnel Management Data Breach," Wikipedia.
- "PennyWise Crypto-Stealing Malware Spreads Through YouTube," Cointelegraph (Spanish).
- "Cobalt Strike: A White Hat Hacker Powerhouse in the Wrong Hands," Cynet.
- "What is a Foothold? A Guide to Early Intrusion Detection," Huntress Labs.

» La necesidad de utilizar modelos computacionales durante el planeamiento naval

Por TN Lic. Agustín Viera Da Costa [5]

Introducción

La simulación de conflictos armados, con el fin de anticipar los posibles resultados de una contienda, es casi tan antigua como la guerra misma. El término *wargaming* designa a la actividad que busca representar un enfrentamiento bélico mediante tableros, unidades y reglas que modelan su comportamiento.

En la actualidad, el constante desarrollo de los medios de combate obliga a complementar el wargaming tradicional con modelos computacionales. Estas herramientas, basadas en principios matemáticos, tienen como objetivo reducir la incertidumbre y convertirse en apoyo concreto para la toma de decisiones del comando. Tal como señala el *Navy Warfare Publication 5-01*, el planeamiento requiere integrar "herramientas que permitan explorar modos de acción bajo condiciones realistas de fricción e incertidumbre".

Modelos computacionales en wargaming

El tablero, los dados y el lápiz resultaron suficientes durante siglos para ensayar conflictos militares. Sin embargo, la incorporación de nuevas tecnologías al campo de batalla volvió insuficiente esa práctica. Hoy, las fórmulas matemáticas y las simulaciones Monte Carlo permiten recrear miles de escenarios en apenas segundos, otorgando al planificador la posibilidad de evaluar distintos cursos de acción en tiempo reducido.

[5] Teniente de Navío. Licenciado en Recursos Navales para la Defensa.

La principal ventaja radica en que el decisor no obtiene un único resultado, sino una **distribución probabilística** de posibles desenlaces. En palabras de Clausewitz, la guerra es "el reino de la incertidumbre"; los modelos computacionales permiten cuantificar esa incertidumbre y transformarla en un insumo para la conducción táctica.

Como lo adelantó Christy en su estudio sobre la aplicación de las Leyes de Lanchester a maniobras de pequeñas unidades, "probabilistic and mathematical investigations of small unit tactics can at least open unknown doors"[1].

Figura 1A – Panel Principal del Comparador mostrando parámetros de entrada.

La fricción táctica y su modelado computacional

La guerra nunca se desarrolla tal como fue planeada. Factores como el clima, el desgaste de los sistemas, las limitaciones logísticas o el error humano generan lo que Clausewitz denominó *fricción*: la diferencia entre la guerra "en el papel" y la guerra "en la realidad".

La ciencia militar, consciente de este desafío, ha comenzado a aplicar modelos que introducen fricción de manera controlada. De este modo, el comandante puede ensayar escenarios donde se simula el impacto de condiciones adversas (por ejemplo, mala propagación acústica en operaciones antisubmarinas, o el desgaste de sensores de vigilancia aérea) sin necesidad de exponer medios reales a dichas situaciones.

Parámetro	Descripción operativa	Mínimo sugerido	Máximo sugerido	Ejemplo de efecto
W_O	Ponderación del atributo ofensivo en el cálculo del poder combinado.	0,1	0,5	↑ resalta misiles/artillería ofensiva.
W_D	Peso relativo de la defensa (blindaje, contramedidas, defensa aérea).	0,1	0,4	↑ hace más relevantes a buques con AA/defensas.
W_I	Peso del impacto (letalidad al infligir bajas decisivas).	0,2	0,4	↑ refleja misiles de gran letalidad (Harpoon, Exocet).
W_R	Peso de la resistencia (capacidad de mantenerse en combate).	0,05	0,2	↑ favorece unidades con durabilidad y autonomía.
COMB_FUNC	Función matemática de combinación de atributos.	—	—	Normalmente se deja en "POND_MEDIA".
SINERGIA_A	Incremento doctrinal por cooperación táctica argentina.	0	0,2	↑ si se busca reflejar interoperabilidad Azul (corbeta + avión patrulla).
SINERGIA_B	Incremento doctrinal por cooperación táctica chilena.	0	0,5	↑ refleja coordinación de plataformas de Rojo (submarino + fragata).
SATURACION_K	Factor de saturación: penaliza la eficiencia al concentrar demasiadas unidades.	0,7	1	Con 0,70 → ataques masivos pierden mucha efectividad; con 1,00 → no hay penalización.
EFICIENCIA_GAMMA	Modificador global de eficiencia doctrinal (entrenamiento, C2, disciplina).	0,8	1	↑ representa fuerzas bien entrenadas, ↓ refleja fricción doctrinal.

Figura 2 – Panel de control para introducir factores de fricción táctica: degradación de sensores, condiciones ambientales y sinergia entre unidades.

El caso del Comparador de Unidades de Combate

Un ejemplo concreto lo constituye el **Comparador de Unidades de Combate**, herramienta informática desarrollada sobre la base de las Leyes de Lanchester y simulaciones Monte Carlo. Su finalidad es representar enfrentamientos entre unidades navales, aéreas y submarinas, integrando variables ofensivas, defensivas y ambientales para estimar probabilidades de éxito.

El enfoque se alinea con modelos previos aplicados a la guerra naval, donde se concluyó que "la superioridad numérica no garantiza la victoria, pues factores como la maniobra y la calidad de sensores alteran la ecuación"[2].

En términos prácticos, el Comparador permite ensayar modos de acción (MA). Por ejemplo, simular un enfrentamiento entre una corbeta misilística y un avión de ataque: lejos de ofrecer un único veredicto, el modelo revela un abanico probabilístico donde puede observarse, en determinado porcentaje de iteraciones, la pérdida de la unidad aérea, y en otro, la de la corbeta. Esta información, lejos de ser concluyente, nutre el juicio del comandante con tendencias y umbrales de riesgo.

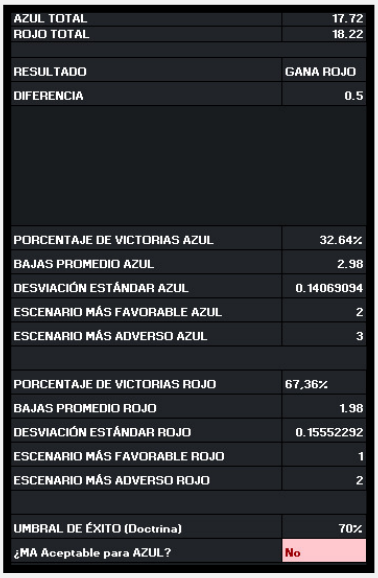


Figura 1B – Resultados probabilísticos obtenidos tras 10.000 iteraciones de simulación Monte Carlo, mostrando distribución de escenarios favorables y desfavorables.

Un ejemplo práctico

En primer lugar, se seleccionan las unidades que participarán en la simulación. En el ejemplo, un bando cuenta con un Destructor tipo MEKO 360 y dos Corbetas tipo MEKO 140, mientras que el otro dispone de una fragata Type 22 y una Type 23 (Figura 1A).

Una vez definidas las unidades, al pulsar el botón **"Comparador Total Atributos"** el sistema calcula el poder de combate relativo de las fuerzas enfrentadas, aplicando la Ley de los Cuadrados de Lanchester. El resultado, de carácter determinístico, se muestra en el margen superior derecho del panel principal (Figura 1A).

Para introducir la fricción táctica, la herramienta incorpora una segunda función: ejecutar miles de iteraciones mediante simulaciones Monte Carlo (10.000 en este ejemplo). El producto es un análisis probabilístico que permite explorar múltiples escenarios en apenas minutos, cuyos resultados se presentan en la Figura 1B.

Finalmente, con el fin de acercar el modelo aún más a la realidad operativa, el Comparador dispone de un panel específico para variar condiciones como la degradación de sensores o la sinergia entre unidades (Figura 2). La base de datos de fuerzas, organizada en una matriz de unidades, se observa en la Figura 3.

UNIDAD	FUERZA	ROL	O_IND_M	O_IND_SD	O_CONJ_M	O_CONJ_SD	D_IND_M	D_IND_SD	D_CONJ_M	D_CONJ_SD	I_IND_M	I_IND_SD	I_CONJ_M	I_CONJ_SD	R_IND_M	R_IND_SD	R_CONJ_M	R_CONJ_SD	FUENTE	FECHA_CALIB	OBS
TYPE 209/1200	CUALQUIERA		90	5	90	5	50	5	50	5	0,8	0,05	0,8	0,05	100	15	100	15			
TR1700	CUALQUIERA		90	5	90	5	50	5	50	5	0,8	0,05	0,8	0,05	100	15	100	15			
MEKO 360 H2 DDGHM	CUALQUIERA		85	5	85	5	65	5	65	5	0,75	0,05	0,75	0,05	80	12	80	12			
TYPE A69 FFG	CUALQUIERA		60	10	60	10	50	5	50	5	0,6	0,05	0,6	0,05	60	9	60	9			
MEKO140 A16 FFGH	CUALQUIERA		60	10	60	10	50	5	50	5	0,6	0,05	0,6	0,05	60	9	60	9			
AS 555 SN FENNEC	CUALQUIERA		40	10	40	10	20	5	20	5	0,55	0,1	0,55	0,1	40	6	40	6			
SUPER ETENDARD	CUALQUIERA		75	10	75	10	30	5	30	5	0,7	0,05	0,7	0,05	40	6	40	6			
ASH-3H SEA KING	CUALQUIERA		40	10	40	10	20	5	20	5	0,55	0,1	0,55	0,1	40	6	40	6			
UH-3H SEA KING	CUALQUIERA		40	10	40	10	20	5	20	5	0,55	0,1	0,55	0,1	40	6	40	6			
TRACKER	CUALQUIERA		75	10	75	10	30	5	30	5	0,7	0,05	0,7	0,05	40	6	40	6			
LOCKHEED P-3B ORION	CUALQUIERA		75	10	75	10	30	5	30	5	0,7	0,05	0,7	0,05	40	6	40	6			
BEECHCRAFT B200 CORMORAN	CUALQUIERA		75	10	75	10	30	5	30	5	0,7	0,05	0,7	0,05	40	6	40	6			
TYPE TNC45 INTRÉPIDA	CUALQUIERA		35	10	35	10	25	5	25	5	0,5	0,1	0,5	0,1	40	6	40	6			
TYPE 42 CLASS LCC	CUALQUIERA		90	5	90	5	70	5	70	5	0,78	0,05	0,78	0,05	100	15	100	15			
DURANCE AORH	CUALQUIERA		0	0	0	0	15	5	15	5	0	0	0	0	60	9	60	9			
COSTA SUR (TRANSPORT)	CUALQUIERA		0	0	0	0	10	5	10	5	0	0	0	0	40	6	40	6			
ICEBREAKER (AGB/AGOP)	CUALQUIERA		0	0	0	0	10	5	10	5	0	0	0	0	40	6	40	6			
LANCHA PATRULLERA CLASE "BARADERO"	CUALQUIERA		35	10	35	10	25	5	25	5	0,5	0,1	0,5	0,1	40	6	40	6			
PATRULLERO OCEÁNICO CLASE GOWIND	CUALQUIERA		45	5	45	5	35	5	35	5	0,55	0,05	0,55	0,05	60	9	60	9			
SCORPENE CLASS	CUALQUIERA		90	5	90	5	50	5	50	5	0,8	0,05	0,8	0,05	100	15	100	15			
TYPE 209/1400	CUALQUIERA		90	5	90	5	50	5	50	5	0,8	0,05	0,8	0,05	100	15	100	15			
BLANCO ENCALADA (M) FFGHM	CUALQUIERA		85	5	85	5	65	5	65	5	0,75	0,05	0,75	0,05	80	12	80	12			
LATORRE J. V. HEMMSKERCK FFGM	CUALQUIERA		85	5	85	5	65	5	65	5	0,75	0,05	0,75	0,05	80	12	80	12			
BROADSWORD CLASS TYPE 22 FFHM	CUALQUIERA		85	5	85	5	65	5	65	5	0,75	0,05	0,75	0,05	80	12	80	12			
COCHRANE CLASS TYPE 23 FFGHM	CUALQUIERA		85	5	85	5	65	5	65	5	0,75	0,05	0,75	0,05	80	12	80	12			
BELL 206B JET RANGER	CUALQUIERA		40	10	40	10	20	5	20	5	0,55	0,1	0,55	0,1	40	6	40	6			
EUROCOPTER NAS 332 C COUGAR	CUALQUIERA		40	10	40	10	20	5	20	5	0,55	0,1	0,55	0,1	40	6	40	6			
AS-365 N2/AS 365 F1	CUALQUIERA		40	10	40	10	20	5	20	5	0,55	0,1	0,55	0,1	40	6	40	6			
MBB BO105C	CUALQUIERA		40	10	40	10	20	5	20	5	0,55	0,1	0,55	0,1	40	6	40	6			
EMBRAER EMB-111 BANDEIRANTE	CUALQUIERA		75	10	75	10	30	5	30	5	0,7	0,05	0,7	0,05	40	6	40	6			
EUROCOPTER AS 332L SUPER PUMA	CUALQUIERA		40	10	40	10	20	5	20	5	0,55	0,1	0,55	0,1	40	6	40	6			
LOCKHEED P-3A ORION	CUALQUIERA		75	10	75	10	30	5	30	5	0,7	0,05	0,7	0,05	40	6	40	6			
EADS CASA C-295 PERSUADER	CUALQUIERA		75	10	75	10	30	5	30	5	0,7	0,05	0,7	0,05	40	6	40	6			
SAAR 4 CLASS CASMA	CUALQUIERA		55	10	55	10	30	5	30	5	0,65	0,1	0,65	0,1	40	6	40	6			
PILOTO PARDO CLASS	CUALQUIERA		45	5	45	5	35	5	35	5	0,55	0,05	0,55	0,05	60	9	60	9			
MAIPO (BATRAL) CLASS LSTH	CUALQUIERA		20	10	20	10	40	5	40	5	0,4	0,1	0,4	0,1	80	12	80	12			
FOUDRE CLASS LSDH	CUALQUIERA		20	10	20	10	40	5	40	5	0,4	0,1	0,4	0,1	80	12	80	12			
AOR ALMIRANTE MONTT	CUALQUIERA		0	0	0	0	15	5	15	5	0	0	0	0	60	9	60	9			
AOR ARAUCANO	CUALQUIERA		0	0	0	0	15	5	15	5	0	0	0	0	60	9	60	9			
TRANSPORT SHIP APH	CUALQUIERA		0	0	0	0	10	5	10	5	0	0	0	0	40	6	40	6			

Figura 3 – Matriz que organiza las unidades disponibles para la simulación.

Conclusión

El propósito de los modelos computacionales aplicados al wargaming no es "predecir la guerra", sino comprender las posibilidades y límites de acción. Estos modelos permiten ensayar, en cuestión de minutos, escenarios que en el terreno exigirían un alto costo de tiempo, medios y riesgo.

El **Comparador de Unidades de Combate** demuestra cómo la iniciativa personal y la aplicación de métodos cuantitativos pueden aportar valor tangible al planeamiento y la enseñanza naval. Tal como recuerda el *ALLIED TACTICAL PUBLICATION (ATP-1)*, la preparación del comandante exige entrenar su capacidad de decisión en contextos de incertidumbre.

La validez de este enfoque no es teórica: ya en 1989, Wang desarrolló el *System Performance Simulation (SPS)* en la Naval Postgraduate School, demostrando que "the anti-air-warfare oriented SPS is a probabilistic event store computer simulation [...] developed as a Monte Carlo computer simulation"[3].

La cuestión entonces no es si debemos incorporar modelos computacionales al planeamiento naval, sino:

¿Podemos permitirnos prescindir de una herramienta que nos entrena para enfrentar la fricción del mañana con mayor claridad en la decisión de hoy?

Notas

1. Christy, D. (1969). *Lanchester and Maneuver: A Study in Small Unit Tactics*. Naval Postgraduate School.
2. *Modelo de Batalla Naval*. Aplicación de las Leyes de Lanchester a enfrentamientos navales.
3. Wang, K.-M. (1989). *A Simulation of Ship Survivability Versus Radar Detection Ranges Against Low Flying Target*. Naval Postgraduate School.

» Concienciación en ciberseguridad para la preservación del poder de combate

Por TN Lic. Maximiliano Daniel Gamboa[6]

Introducción

En el artículo anterior, donde es habló sobre Ingeniería Social, conceptualizamos al ciberespacio y los vectores de ataque de los cuales el personal naval puede ser víctima. Además de lo mencionado, se presentaron ejemplos de la aplicación de la Ingeniería Social sobre blancos militares para el apoyo de operaciones en el terreno, robo de información, entre otros.

De todo lo visto, se concluyó que, para asegurar el poder naval, no basta con proteger la integridad física de las plataformas o sistemas, sino que es indispensable salvaguardar la capacidad de tomar decisiones, frente a las acciones de actores maliciosos en el ciberespacio.

En este contexto, avanzaremos en la caracterización de otro tipo de amenazas que se presenta en el ciberespacio: el MALWARE.

¿Qué es el Malware?

El término conocido como "malware" tiene su origen en la combinación de dos elementos: "malicious" y "software", y por esa razón también es conocido como "software malicioso". Este término incluye a todos aquellos softwares diseñados para causar daño, o realizar actividades no autorizadas por los usuarios legítimos.

Las motivaciones que puede tener un adversario, para infectar un sistema con un malware, son de las más variadas, y en este sentido el instrumento militar puede verse comprometido en diferentes

[6] Teniente de Navío. Licenciado en Recursos Navales para la Defensa.

formas: exfiltración de información sensible, campañas persistentes de espionaje, sabotaje informático y manipulación de sistemas, denegación de servicios, entre otras.

Las organizaciones militares, pueden ser víctimas de diferentes amenazas, tales como estados hostiles, grupos de crimen organizado u organizaciones hacktivistas[7].

Tipos de Malware

Los softwares maliciosos se diferencian entre sí, en función de sus características técnicas, los objetivos de su diseño y la forma en la que operan dentro de los sistemas (Fig. N° 1). En base a ello, se diferencian, y existen, múltiples formas de malware. Las más comunes son:

- Virus: Un virus es una porción de código, dentro de un software, que al ejecutarse lleva a cabo las actividades maliciosas para la que fue diseñado. Su nombre se debe a la forma de actuación y de propagación que tiene este malware.

Un virus suele propagarse dentro de una red de ordenadores por medio del traspaso de documentación. Otra forma en la que un sistema puede verse afectado es por medio de la navegación en sitios infectados por virus, o descargas de archivos adjuntos de sitios web, correos electrónicos, u otras fuentes.

Vale mencionar que, un virus suele estar inactivo hasta que la aplicación, o software que lo contiene, es ejecutado. A partir de ese momento el virus se desplegará en el sistema y llevará a cabo los cometidos por los que fue concebido y se replicará a sí mismo. (Karspersky LATAM, s.f.)

- Gusanos (Worms): Los gusanos son un tipo de malware que se propaga en las redes informáticas explotando las vulnerabilidades del Sistema Operativo. A diferencia del virus informático, el cual se aloja en una aplicación hasta su ejecución, el gusano es un programa independiente que se replica y se propaga dentro de una red de equipos infectándolos.

Un gusano, generalmente suele contener una carga útil para dañar a los sistemas, por lo que los adversarios suelen explotar la capacidad de un gusano de replicarse y propagarse, para obtener una entrada a los dispositivos y explotar las vulnerabilidades.

El proceso de autorreplicación de un gusano, dentro de un ordenador, se suele manifestar en la saturación de los recursos, ocasionando que la computadora se ralentice o funcione inapropiadamente.

- Troyanos (Trojans): Un troyano es un malware que aparenta ser un software legítimo, con el propósito de engañar al usuario e inducirlo a descargarlo y ejecutarlo. De esta forma el malware ingresa a los sistemas y despliegan sus cargas útiles.

A diferencia de un gusano, necesitan un host para funcionar. Una vez que el troyano se instala en un dispositivo, los piratas informáticos pueden usarlo para eliminar, modificar o capturar datos, recolectar su dispositivo como parte de un botnet[8] u obtener acceso a su red.

- Ransomware: El ransomware es un tipo de malware que se caracteriza por cifrar los archivos del sistema afectado y, a raíz de esto, se suele exigir un rescate económico para restaurar el acceso. En su aplicación militar, puede llegar a omitirse esta última característica, porque es una práctica muy común entre los ciberdelincuentes. Si bien, un

[7] Hacktivismo: es el uso de técnicas de hacking con el objetivo de promover causas políticas, sociales o ideológicas, en lugar de obtener beneficios económicos.
[8] Botnet (abreviatura de "robot network"): Es una red de computadoras infectadas con malware que son controladas remotamente por un atacante. Estas máquinas infectadas, conocidas como "bots" o "zombies", pueden ser utilizadas para realizar ataques cibernéticos a gran escala, como ataques DDoS, entre otros.

ransomware es más conocido por cifrar los datos de los objetivos, también pueden utilizarse para bloquear acceso a sistemas.

Generalmente, se transmite como un troyano o un gusano y luego de ello se encarga de infectar el Sistema Operativo, explotando vulnerabilidades conocidas. Siempre dependerá de que el usuario, o víctima, lleve a cabo la acción de ejecución.

- **Spyware:** El Spyware es una forma de malware que, una vez en el sistema del objetivo, se encarga de controlar la actividad, robar credenciales, datos personales, registrar pulsaciones de teclado, registrar ubicación y otros, según como esté programado.

Puede ser instalado en un sistema mediante diferentes vectores: descargas desde sitios web maliciosos, dar "click" en enlaces engañosos, instalación de aplicaciones falsas, entre otras.

- **Adware:** El adware es un malware que genera que se muestren anuncios no deseados, o sitios web de anuncios, en un sistema o dispositivo móvil. Lo que hace es redirigir los resultados de las búsquedas a sitios web de publicidad y recopilar datos de los usuarios para, luego, venderlo a anunciantes web.
- **Rootkits:** Un rootkit es un conjunto de herramientas que permite el acceso privilegiado a un sistema, ocultando su presencia y la de otros malwares. Puede manipular el sistema operativo para no ser detectado por antivirus o herramientas de monitoreo, convirtiéndose en una amenaza persistente y difícil de eliminar.
- **Keyloggers:** Los keyloggers son un tipo de spyware que monitorea la actividad del usuario, registrando las pulsaciones de las teclas de un dispositivo, sin conocimiento del usuario.

Vectores de Ingreso Comunes

Los vectores de ingreso son los medios por los cuales el malware logra acceder a un sistema (Fig. N° 1). A continuación, se enumeran los más frecuentes:

- **Correos Electrónicos de Phishing**: Uno de los métodos más comunes y efectivos. Los atacantes envían correos que simulan ser legítimos, conteniendo enlaces maliciosos o archivos adjuntos infectados.
- **Descargas desde Sitios No Seguros:** Muchas veces, los usuarios descargan software desde fuentes no oficiales o sitios pirata que incluyen malware oculto. Esto incluye juegos crackeados[9], herramientas de productividad y hasta supuestas actualizaciones de sistema.
- **Dispositivos Externos Infecciosos:** Los dispositivos USB's o discos externos pueden estar infectados y, al conectarse, ejecutar código malicioso automáticamente si el sistema está mal configurado. Esta técnica es común en ataques dirigidos.
- **Redes Wi-Fi Inseguras:** Conectarse a redes Wi-Fi públicas o no cifradas puede exponer al usuario a ataques del tipo man-in-the-middle[10], en los que el atacante intercepta el tráfico y puede inyectar malware en tiempo real.
- **Vulnerabilidades del Sistema o Software Desactualizado:** Muchos ataques aprovechan vulnerabilidades conocidas en sistemas operativos, navegadores o programas. Si no se aplican actualizaciones de seguridad, se convierten en puertas abiertas para los atacantes.

[9] **Crackeado**: Refiere a aquellos softwares para los que se desarrollan parches sin autorización del desarrollador del programa para de modificar el comportamiento del software original.
[10] **Man In The Middle (MitM)**: Tipo de ciberataque en el que un atacante se posiciona entre dos usuarios que se están comunicando, interceptando, espiando y potencialmente modificando la información intercambiada.

- **Ingeniería Social:** Tácticas de manipulación psicológica para convencer al usuario de que ejecute un archivo malicioso o brinde acceso a información crítica. Esta técnica no requiere habilidades técnicas avanzadas, solo astucia y conocimiento del comportamiento humano.
- **Aplicaciones Móviles Maliciosas:** En dispositivos móviles, las apps descargadas fuera de tiendas oficiales (APK[11] en Android, por ejemplo) pueden contener malware. Incluso algunas apps en tiendas legítimas han sido descubiertas como maliciosas tras pasar filtros de seguridad.

Figura N° 1: Tipos de Malwares y vectores de ingreso

Medidas de Prevención y Protección

La prevención sigue siendo la mejor defensa contra el malware. Algunas buenas prácticas incluyen:

- **Mantener el software actualizado:** Aplicar parches de seguridad en cuanto estén disponibles.
- **Uso de antivirus y herramientas antimalware confiables:** Con bases de datos actualizadas y escaneos periódicos.
- **Cuidado con los correos electrónicos sospechosos:** No abrir enlaces ni descargar archivos de remitentes desconocidos.
- **Descargar software solo desde fuentes oficiales:** Evitar páginas de dudosa reputación.
- **Uso de contraseñas robustas y autenticación multifactor (MFA):** Para evitar accesos no autorizados.
- **Realizar copias de seguridad regularmente:** Para minimizar el impacto en caso de ataque.

[11] **APK (Android Package Kit):** Es el formato de archivo utilizado para distribuir e instalar aplicaciones móviles en dispositivos Android.

- **Educación y concienciación del usuario:** El factor humano sigue siendo la primera línea de defensa y, a la vez, el eslabón más débil.

Riesgos para las organizaciones navales.

Hasta ahora, hemos visto que es un malware, cuales son los diferentes tipos, como ingresan a un sistema para su infección, y como podemos hacer para prevenirlo. Asimismo, y como se dijo en la introducción al presente artículo, debemos tener en cuenta que una organización naval se compone tanto de sus recursos materiales, como de sus recursos humanos, por ello es importante diferenciar los sistemas que pueden ser afectados por estos malwares.

Hoy en día, uno puede encontrar mucha información pública sobre los diferentes tipos de malwares que afectan a organizaciones civiles, de modo que una gran comunidad de organizaciones colabora para alimentar esa fuente de conocimiento sobre, amenazas, vulnerabilidades y ciberarmas, pero esto solo cubre una parte de los riesgos a los que está expuesta una organización naval.

En general, una organización naval, como cualquier otra organización militar, tiene sistemas y redes que utilizan softwares propietarios, a los que se puede acceder a través de internet, o en forma remota, y otros sistemas que operan en forma aislada, o cerrada, sobre redes desconectadas físicamente de internet, conocidos como "air-gapped systems".

a. Sistemas Conectados a Redes Externas: Vulnerabilidades y Riesgos

En el caso de aquellos sistemas y redes mencionados en primera instancia, especialmente los que se conectan a través de internet, resulta necesaria la aplicación de tecnologías de seguridad que impidan el acceso de actores maliciosos, y especialmente buenas prácticas de ciberseguridad por parte de los operadores. Que un servicio se pueda conectar a través de internet facilita la tarea de reconocimiento de vulnerabilidades por parte de adversarios, quienes pueden utilizar técnicas de Open Source Intelligence (Inteligencia de fuentes abiertas - OSINT) para recolectar información sobre configuraciones visibles (como servicios, versiones, puertos abiertos). De esta forma, es mucho más sencillo emplear un malware apropiado para cada vulnerabilidad detectada en la etapa de reconocimiento. Por esta razón, es importante una adecuada política de seguridad para la utilización de los servicios de la Armada a los que se puede ingresar de forma remota.

De esta forma, podemos obtener un conocimiento más acabado de las razones por las cuales se pueden dar incidentes de exfiltración de información en organizaciones militares, sobre todo parte de su infraestructura se encuentra alojada en servidores externos, cuando están conectadas a internet, o cuando tienen servicios de ciberseguridad tercerizados. Cuando se conjugan este tipo de cuestiones, un atacante puede explotar una vulnerabilidad descubierta en el proveedor de ciberseguridad, y sacar provecho de ello con fines maliciosos.

Un ejemplo de esto fue lo acontecido en la Marina de los Estados Unidos (USN), y a otras agencias de defensa, cuando en febrero de 2025 salió a la luz que sus sistemas habían sido comprometidos por un malware que recopilaba información (también conocidos como "infostealers"). En esta situación, 30 empleados de la USN habrían accedido a sitios donde descargaron este malware el cual podría estar camuflado en archivos PDF, parches para videojuegos, u otros medios, y al ejecutar el archivo infectaron la computadora que usaban para trabajar. De esta forma, el malware comenzó a exfiltrar información sobre credenciales de acceso, autenticación multifactor[12], credenciales de inicio de sesión de mail, documentación, cookies de inicio de sesión, entre otros. Estos datos fueron robados y ofrecidos en foros de venta de información ilegal, con los riesgos que

[12] **Autenticación Multifactor (MFA)**: Proceso de inicio de sesión que requiere más que una simple contraseña para verificar la identidad de un usuario

ello conlleva para la Seguridad Nacional (Gal, 2025). Aunque este incidente no fue reconocido oficialmente, la información ofrecida en foros de la dark web[13], así permitieron asumirlo.

b. Sistemas Aislados (Air-Gapped): Retos para los Atacantes

En el caso de aquellos sistemas aislados, y frente a la imposibilidad de acceder en forma remota para interactuar con ellos, estos representan un desafío aún mayor para los atacantes. Frente a esto, un enemigo debe llevar a cabo una investigación profunda de los subsistemas que componen al sistema objetivo, las formas de ingreso y los posibles vectores de ataque, de lo contrario no habrá posibilidad de infectar con malware al mismo.

Esta preocupación fue presentada por el U.S Government Accountability Office (GAO) en un informe presentado al Senado de los EE.UU. en octubre del año 2018, en el cual hablaba sobre la ciberseguridad de los Sistemas de Armas del Departamento de Defensa (DoD) y, en particular, expresaba la necesidad de revisar las medidas de ciberseguridad de los buques de guerra, dado que los mismos utilizan sistemas de control industrial para su propulsión, haciendo énfasis en la falta de controles de seguridad que los mismos poseían hasta entonces (GAO, 2018).

En las Unidades Navales Modernas los sistemas suelen estar segmentados entre aquellos que son necesarios para el gobierno de la unidad, los necesarios para la navegación y los de servicio, estos último generalmente necesitan de conexión a internet.

Para el caso de un ataque por malware a una Unidad Naval, el atacante debería de conocer en profundidad el sistema con el que cuenta la misma y sus vulnerabilidades, lo cual, por tratarse de un sistema aislado, requiere de acceso físico al mismo o de la existencia de una puerta trasera[14] que pueda llegar a ser identificada por el enemigo.

Como norma general, se suele decir que, si alguien quiere proteger algo, no debe conectarlo a internet. Cuando los sistemas no están conectados a internet, se disminuyen muchísimo las posibilidades de que un agente externo pueda llevar a cabo un ataque con infección de malware en forma remota, ya que para poder infectar al Software de Supervisión, Control y adquisición de Datos (SCADA[15]), que reúne la información del funcionamiento de los sensores de una unidad, se requiere acceso físico al mismo, debiendo saltear controles físicos y lógicos para alterar el funcionamiento de los sistemas de propulsión, hidráulicos, de dirección y otros sistemas críticos (Fig. N°2). No obstante, existen métodos de securización para este tipo de sistemas, que es parte del campo de la Ciberseguridad OT (Operational Technology[16]).

[13] **Dark Web**: Parte de Internet que no está indexada por los motores de búsqueda convencionales y que requiere software especializado, como Tor, para acceder

[14] **Puerta trasera (backdoor):** mecanismo que permite a un usuario no autorizado acceder a un sistema, evadiendo los mecanismos de seguridad habituales. Puede ser una vulnerabilidad en el software, un error de código o una característica añadida a propósito.

[15] **SCADA**: Es sistema de software y hardware que permite a las organizaciones industriales controlar, supervisar y adquirir datos en tiempo real de sus procesos y equipos.

[16] OT hace referencia a los sistemas de control industrial que gestionan procesos físicos.

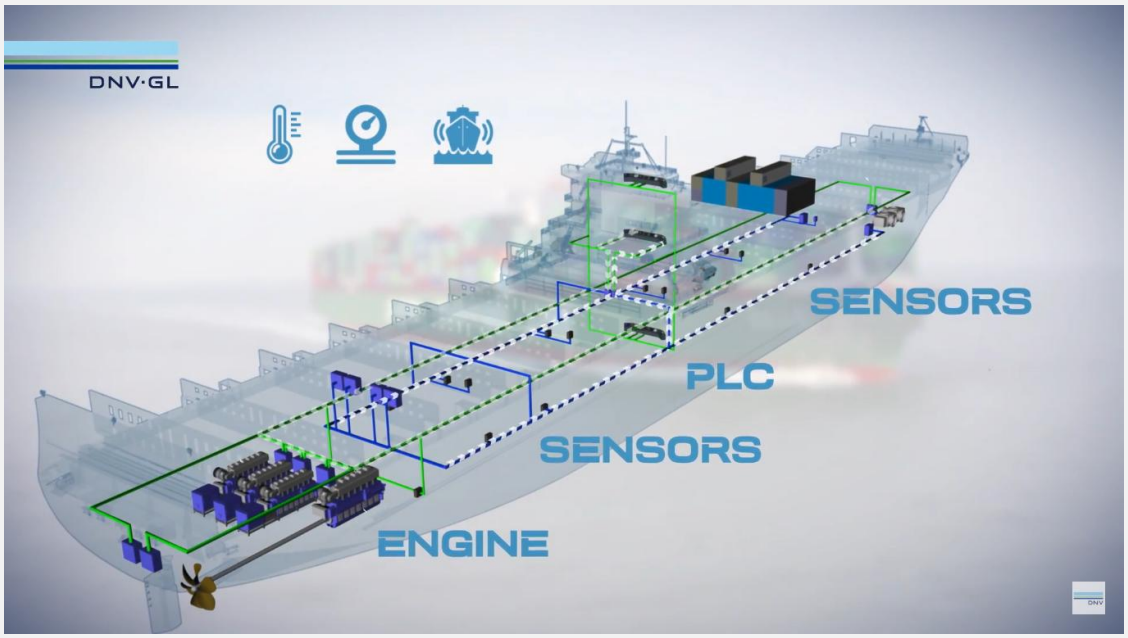


Figura N° 2: Tipo de configuración de dispositivos OT en una unidad naval moderna[17].

Si bien, no hay casos documentados de Unidades Navales que hayan sido afectadas por este tipo de ataques, los mismos siguen siendo una preocupación a raíz de los antecedentes ocurridos en otras industrias. Un ejemplo bien conocido de ello fue lo acontecido con el virus "Stuxnet".

Stuxnet fue un malware altamente sofisticado descubierto en 2010, diseñado específicamente para sabotear el programa nuclear iraní mediante la manipulación encubierta de sistemas SCADA y la información provista por los dispositivos OT. Infectaba computadoras Windows utilizando múltiples vulnerabilidades zero-day y se dirigía a PLC para alterar el funcionamiento de las centrifugadoras de enriquecimiento de uranio sin alertar a los operadores.

Los comandos PLC[18], que constituían una de las cargas útiles principales de STUXNET, estaban diseñados para ejecutarse únicamente en sistemas con configuraciones de hardware muy específicas, por lo que los atacantes tenían conocimiento detallado de la configuración específica del sistema objetivo.

Por otro lado, los sistemas industriales bajo control SCADA atacados por STUXNET podrían resultar dañados o completamente destruidos, dependiendo de los comandos modificados enviados por los atacantes. De esta forma se lograba modificar la velocidad de rotación de las centrifugadoras, causando daños físicos progresivos mientras mostraba lecturas normales en el sistema, lo que derivó en la destrucción de aproximadamente 1.000 unidades en la planta de Natanz.

Stuxnet marcó un hito como la primera ciberarma conocida que logró un efecto físico sobre una infraestructura crítica, evidenciando la vulnerabilidad de los sistemas industriales y transformando el enfoque global hacia la ciberseguridad en entornos SCADA y OT, por lo cual es una amenaza latente en todos aquellos sectores que emplean estas tecnologías.

Conclusión

El malware representa una de las mayores amenazas en el ámbito de la ciberseguridad. Su evolución constante y la creatividad de los atacantes hacen que ningún sistema esté

[17] Imagen recuperada de material audiovisual. https://www.youtube.com/watch?v=P0F30xcDFQg
[18] **Programmable Logic Controller (PLC):** Es un dispositivo electrónico digital que se utiliza para automatizar procesos industriales. Los PLC se utilizan para controlar una amplia gama de procesos industriales, como el control de máquinas, la automatización de líneas de producción, la gestión de sistemas de iluminación y climatización, entre otros.

completamente a salvo. Por ello, conocer los distintos tipos de malware y los vectores por los cuales acceden a nuestros sistemas es esencial para desarrollar una defensa sólida y efectiva.

Invertir en prevención, educar a los usuarios y mantenerse actualizado son pasos indispensables en la lucha contra este enemigo invisible pero omnipresente. En un entorno donde los datos son el recurso más valioso, protegerlos debe ser una prioridad constante.

Asimismo, resulta indispensable conocer las vulnerabilidades de los diferentes sistemas que se encuentran presentes en las Unidades Navales y en los entornos de trabajo que se utilizan diariamente, como así también la aplicación de auditorías internas y campañas de concienciación para reducir los riesgos asociados al mal uso de los servicios tecnológicos.

Bibliografía

Buxton, O. (20 de diciembre de 2024). *Norton*. Recuperado el 28 de abril de 2028, de US Norton: https://us.norton.com/blog/malware/types-of-malware

CICR. (2024). *¿CUÁL ES LA DEFINICIÓN*.

GAO. (2018). *Weapon System Cybersecurity*.

Karspersky LATAM. (s.f.). *Karspersky*. Recuperado el 22 de abril de 2025, de Karspersky: https://latam.kaspersky.com/resource-center/threats/types-of-malware?srsltid=AfmBOorC1xbk-1uQszeZwbsPFFwNrDPPPYdBrjcPzqb-BWlQOXmLbWBf

Velluz, D. (octubre de 2010). El malware STUXNET ataca los sistemas SCADA. *TrendMicro*. Recuperado el 24 de mayo de 2025, de https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems

.

» Ciberespacio y Ciberguerra: Comprendiendo las acciones en el 5to dominio y su interacción en las Guerras Híbridas.

Por TN Lic. Maximiliano Daniel Gamboa[19]

Introducción.

En este artículo vamos a abordar las peculiaridades del ciberespacio, la ciberguerra y lo vamos a relacionar con el concepto de guerra híbrida, pero antes de adentrarnos en esta tarea debemos comenzar con aclarar algunos conceptos. El primero de ello es la comprensión de qué es la de Guerra, para lo que es necesario asumir que éste es un fenómeno muy antiguo, y prácticamente la historia de la humanidad está atravesada por él.

Aristóteles, por ejemplo, definía a la guerra como una herramienta para alcanzar la paz, y en cierta forma Vegecio, pensador militar romano, coincidía con este punto de vista, aunque argumentando que para llevar a cabo esta empresa hacía falta una gran preparación y entrenamiento. De aquí se desprende la famosa frase "si quieres paz prepárate para la guerra".

Por otra parte, Sun Tzu, pensador oriental, aludía que la cúspide de la guerra consistía en ganarla sin batallar, argumentando que el engaño y la astucia eran las virtudes más importante para ganar una guerra.

Ya en el renacimiento, Maquivalelo postulaba la idea de que la guerra era una actividad intrínsecamente política, necesaria para la supervivencia y preservación del Estado, no una excepción a la norma. Es uno de los autores más conocidos en abogar por la creación de ejércitos

[19] Teniente de Navío. Licenciado en Recursos Navales para la Defensa.

nacionales de ciudadanos con fuerte disciplina y lealtad en lugar de mercenarios. En su libro "El príncipe", abogaba que era tarea del líder de un país saber todo lo necesario sobre la guerra, tal era la significancia de ésta que un gobernante no podía desconocer como librarla.

Finalmente, arribamos a la versión y definición más conocida por nosotros, la definición de la guerra como una continuación de la política por otros medios. Esta definición, acuñada por Carl Von Clausewitz en su obra "De la Guerra", es la más adoptada por occidente, y es la que marca la doctrina particular de los ejércitos modernos.

No obstante, a pesar de no estar expresado es los ejemplos anteriores, es importante reconocer que la guerra conlleva aplicación violenta de poder. Por ello, debemos comprender, además, que la guerra, en la mayoría de los casos, resulta en un enfrentamiento violento entre partes que se disputan intereses en un escenario específico, y que, además, es un fenómeno social.

Y, ¿por qué hablamos de la guerra como fenómeno social? Esto es así porque involucra a grupos humanos y tiene profundas implicaciones en la estructura social, política y económica de las sociedades, así como en la vida cotidiana de las personas. Es un fenómeno recurrente en la historia de la humanidad y puede ser estudiado a través de disciplinas como la sociología, la polemología y la historia, ya que se manifiesta en patrones, causas y consecuencias que afectan a las comunidades de diversas maneras.

Como fenómeno recurrente en la historia de la humanidad podemos retrotraernos hasta la prehistoria para comprender que, aún en pequeñas sociedades tribales, el enfrentamiento armado era una cuestión de competencia por los recursos. El primer escenario en el que se dieron estos conflictos fue en la tierra, luego en el mar y en el aire, y conforme la tecnología fue avanzando se fueron incorporando nuevos escenarios de combate, hasta llegar a la actualidad y a los escenarios espacial y ciberespacial.

Si bien el ciberespacio comenzó a configurarse con la aparición de las primeras redes informáticas, su operacionalización no fue conceptuada hasta la década del 90', con el advenimiento del internet y la evolución de las tecnologías de la información y la comunicación, tales como evolución en las materias primas, microchips, miniaturización, y otras tecnologías que permitieron esta explosión.

El punto es comprender que, a raíz de la interconectividad, el auge de internet, y la cada día mayor digitalización, la guerra encontró un nuevo escenario: El ciberespacio.

Las características del ciberespacio lo transformaron en un escenario prolífico para el accionar de la criminalidad y el terrorismo. Esto llevo a la militarización de este dominio y al desarrollo de "ciberarmas" aptas para el espionaje y el sabotaje, en pos de garantizar la seguridad e integridad territorial. En este contexto, aparecieron virus como Stuxnet, operaciones como WannaCry, Software espías como Pegasus y otros tantos.

Con todo lo dicho hasta ahora quiero despertar en ustedes la siguiente inquietud: ¿Estamos preparados para la guerra en el ciberespacio? ¿Cuán vulnerables somos en el mismo? ¿de qué tipo de operaciones podemos ser víctimas y no nos damos cuenta? ¿qué paralelismos hay entre las operaciones cinéticas tradicionales y las operaciones en el ciberespacio? Las interrogantes, en este punto, deberían ser muchas, y a lo largo de este artículo iremos desentrañando algunas de ellas.

¿Qué es el Ciberespacio?

Al tratarse de un dominio relativamente novedoso la definición aceptada internacionalmente no existe. Esto se torna aún más complejo desde la aparición de las "ciberarmas" y de la posibilidad de intrazabilidad y anonimato que brinda este dominio para llevar a cabo acciones ofensivas o de

espionaje a nivel estratégico. Estas son solo algunas razones por las cuales aún no existe consenso sobre que es el ciberespacio, que es un ciberataque, que es un "casus belli" en el ciberespacio, que es la soberanía ciberespacial, entre otras cuestiones que son materia del derecho internacional.

En este contexto, nos encontramos con que hay muchas definiciones del ciberespacio, según las doctrinas de diferentes países. Por ejemplo:

España define al ciberespacio como *"el nombre por el que se designa al 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"*

Estados Unidos va un poco más allá y la define como *"Un dominio global dentro del entorno de información (IE) que consiste en redes interdependientes de información infraestructuras tecnológicas y datos de los residentes, incluido el Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados."* incluyendo a los procesadores y controladores integrados como materia de interés del ciberespacio.

El reino unido la define *como "la red interdependiente de infraestructuras de tecnologías de la información que incluye Internet, redes de telecomunicaciones, sistemas informáticos y dispositivos interconectados. Para el ámbito militar, y al considerar nuestros esfuerzos de contrarrestar las amenazas en el ciberespacio, se trata de un dominio operativo, junto con la tierra, el mar, el aire y el espacio."* Se destaca de esta definición que le da al ciberespacio carácter de dominio operativo de interés militar.

Finalmente, nuestro país lo definió en la Estrategia Nacional de Ciberseguridad de 2023 como *"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."* De esta definición se destaca que para nuestro país el ciberespacio tiene carácter transfronterizo y está en constante evolución.

En las definiciones anteriores habrán notado que hay conceptos que se repiten, tanto en forma textual o doctrinal, los cuales son: dominio global – Infraestructuras de tecnología de la información – Internet – Redes e Infraestructuras de telecomunicaciones. Esos términos están referidos a

- Data centers que dan soporte a la nube y al internet.
- Torres y antenas de telecomunicaciones que brindan la posibilidad de conectarse a internet a través de telefonía celular.
- Infraestructura internacional de fibra óptica que permite la globalidad de internet.
- Telepuertos satelitales que brindan la posibilidad de contar con internet satelital en lugares donde la infraestructura no existe o se ve destruida.
- Satélites de comunicaciones.
- Protocolos de comunicación y encriptación.
- Radio propagación, algoritmos, redes de redes (como es el caso de internet).
- PERSONAS, que son quienes interactúan con toda esta infraestructura y tecnologías.

En este sentido, podemos avanzar en la comprensión del Ciberespacio como ese dominio global en el cual prevalecen tres capas que interactúan, necesariamente, entre sí. Hablamos de una capa física, una capa lógica y una capa humana (Figura N°1).

La capa física es aquella que incluye a las redes y los sistemas de información y de telecomunicaciones.

La capa lógica es aquella donde se contemplan los softwares, protocolos y toda aquella solución que implica la comunicación a bajo nivel entre computadoras o sistemas.

Finalmente, la capa humana, que es la que está definida por la relación entre Humano – Sistema.

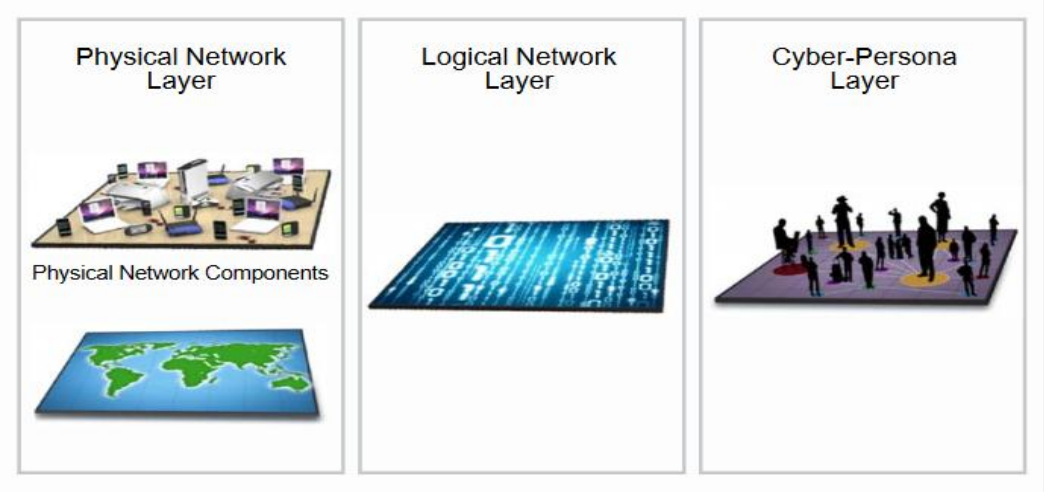


Figura N°1: Capas del Ciberespacio

La importancia de esta introducción reside en aclarar en que consiste el Ciberespacio, tanto lógica como físicamente, dado que para poder atacar o defender algo, es necesario comprenderlo.

Finalmente, vale mencionar que el ciberespacio, en tanto dominio operacional junto al terrestre, marítimo, aéreo y espacial, presenta características propias que exigen una adaptación del pensamiento militar, y representa tanto una superficie de ataque como un centro de gravedad crítico para la conducción de operaciones militares modernas.

La imposibilidad de atacar eficazmente lo que no se comprende resalta la necesidad de una formación específica en ciberdefensa, en particular aquellas de carácter ofensivo, enmarcadas en objetivos militares definidos y bajo principios éticos, legales y estratégicos claros.

Por esta razón, la Ciberdefensa fue institucionalizada en números países, el nuestro entre ellos, para llevar a cabo acciones de Ciberguerra.

¿Qué es la Ciberguerra?

La ciberguerra, tiene varias definiciones. Una de ellas es la de Adam P. Liff, en la que define a la misma como:

"una situación de conflicto entre dos o más actores políticos, caracterizada por la ejecución de ataques deliberados, hostiles y dañinos contra redes de ordenadores en la infraestructura crítica civil o militar de un adversario con intención coercitiva y orientada a la obtención de concesiones políticas; o como una medida de fuerza bruta contra redes militares o civiles con el fin de reducir la capacidad del adversario para defenderse o para llevar a cabo represalias semejantes o mediante fuerzas convencionales, así como contra objetivos militares o civiles con objeto de afectar a un actor por motivos estratégicos"

El escenario principal de la ciberguerra es el ciberespacio, que ha sido reconocido como el quinto dominio, uniéndose a la tierra, el mar, el aire y el espacio.

Características Principales de la Ciberguerra:

- Asimetría: La ciberguerra es el paradigma de la guerra asimétrica. Proporciona los instrumentos necesarios para que actores con pocos recursos puedan enfrentarse, e incluso superar, a potencias mayores con riesgos mínimos, requiriendo solo un ordenador y conocimientos informáticos avanzados. El esfuerzo del defensor es mayor y más costoso que el del atacante, y las naciones más tecno-dependientes son más vulnerables.
- Complejidad y Ocultamiento: Es un fenómeno complejo. La dificultad radica en la identificación y localización del atacante, ya que a menudo no deja un rastro fácil de rastrear, lo que complica la respuesta.
- Rapidez: La velocidad de los cambios en el ciberespacio permite realizar ataques e implementar defensas en muy poco tiempo, a diferencia de las operaciones convencionales. Las ciberarmas tienen una "caducidad muy rápida" debido a la continua evolución tecnológica y de programación.
- Impacto en la Infraestructura Crítica: Un objetivo fundamental de la ciberguerra es la neutralización o el bloqueo de la infraestructura crítica. La relación entre ciberguerra e infraestructura crítica es directa, ya que estas infraestructuras, que son vitales para la sociedad y la seguridad nacional, se convierten en objetivos reales, pudiendo paralizar una nación.

Objetivos y Efectos de la Ciberguerra: Mediante las acciones de ciberguerra se busca lograr diversos objetivos, entre ellos:

- Dañar un sistema o entidad hasta el punto de que no pueda funcionar o ser restaurado sin una reconstrucción completa.
- Interrumpir o romper el flujo de información.
- Destruir físicamente la información del adversario o reducir la efectividad de sus sistemas de comunicación y recolección de información.
- Impedir el acceso y uso de sistemas y servicios críticos.
- Engañar a los adversarios y robarles información.
- Proteger los sistemas propios y restaurar los sistemas atacados.
- Manipular las capacidades de toma de decisiones del enemigo, interfiriendo en la obtención de información útil, degradando sus procesos de resolución y neutralizando sus medios de comunicación. Esto se puede lograr mediante la modificación no autorizada de datos o instrucciones (decepción) o actuando contra las funciones del sistema (manipulación).
- Bloquear la disponibilidad de datos cuando sea necesario.
- Desinformación y manipulación cognitiva.
- Obtención de inteligencia estratégica.

Los ataques de ciberguerra pueden ser lanzados por Estados, organizaciones o incluso individuos. La complejidad aumenta cuando la responsabilidad de los ataques puede recaer en hackers que actúan simultáneamente desde diferentes países y jurisdicciones, complicando la atribución a un Estado.

Tipos de Operaciones en el Ciberespacio:

Para lograr estos objetivos se llevan a cabo diferentes tipos de ciberoperaciones, entre ellas:

- Ciberespionaje: Consiste en el uso de técnicas de infiltración en sistemas enemigos, para la extracción no autorizada de información sensible, propiedad intelectual o datos de sistemas informáticos y redes, con el fin de obtener ventajas políticas, económicas o estratégicas.
- Cibersabotaje: Consiste en aquellos ataques cibernéticos con el objetivo de interrumpir o dañar la infraestructura de una organización, un gobierno o un país. Estos actos pueden afectar la disponibilidad de servicios, la seguridad de la información y la continuidad de las operaciones.
- Ciberpropaganda: Supone controlar la información para influir en la opinión pública. Es un tipo de ciberguerra psicológica que se consigue fácilmente a base de ataques de desinformación en redes sociales y medios digitales, así como a través de "fake news". Con la propaganda, se consigue manipular tanto las opiniones como la conducta de las personas, algo que resulta de gran utilidad en una guerra. De igual modo, las organizaciones terroristas suelen usar este método para reclutar miembros.

Para evitar ser víctima de este tipo de operaciones, se desarrolla la Ciberdefensa de las Infraestructuras Críticas, que consiste en el conjunto de medidas defensivas para proteger la integridad de infraestructuras, sistemas informáticos e infraestructuras de la información, para garantizar la continuación de las operaciones militares.

Guerra Hibrida

La ciberguerra guarda relación con la guerra hibrida, como un instrumento más de ésta.

Recordemos que la guerra híbrida es un concepto que describe una situación de conflicto entre Estados o actores políticos que se caracteriza por la combinación integrada de herramientas militares y no militares, tanto encubiertas como abiertas, que a menudo se lleva a cabo por debajo del umbral de un conflicto armado tradicional o de una guerra formalmente declarada, en lo que se conoce como la "zona gris" entre la paz y la guerra.

Aunque no existe un consenso único sobre su definición, los expertos y organizaciones internacionales suelen referirse a ella como un enfoque estratégico que busca lograr objetivos con un amplio espectro de medios, cinéticos y no cinéticos.

En este contexto, es importante mencionar que toman gran relevancia la asimetría de medios y actores, lo cual se puede materializar en el ciberespacio, mediante acciones de hacking, espionaje y sabotaje a infraestructuras críticas y sistemas de información. En este sentido, la ciberguerra permite que actores con menos recursos se enfrenten a potencias mayores con riesgos mínimos a causa de la posibilidad del anonimato en la red, y usando solo un ordenador y conocimientos informáticos avanzados. Lo interesante de este abordaje es que, en general, el esfuerzo del defensor es a menudo mayor y más costoso que el del atacante.

A lo anterior, se le suma la complejidad en la atribución de un ciberataque, lo que permite que los diferentes actores de amenaza, estatales o patrocinados por estos, puedan operar con un relativo grado de seguridad en cuanto a lo que a responsabilidad se refiere.

Por lo mencionado, el ciberespacio ofrece una gama de posibilidades para los actores de ejecutar ciberoperaciones de diferentes naturalezas.

Amenazas en el Ciberespacio.

Un estado u organización, como la Armada Argentina, puede ser víctima de diferentes tipos de amenazas en el ciberespacio. Entre ellas vamos a distinguir las más relevantes: Las amenazas internas y externas.

En cuanto a las **amenazas internas**, son todas aquellas que tienen alguna relación o vinculación con la organización víctima. En el caso de la Armada Argentina, se pueden identificar como amenazas internas al personal en actividad, el personal retirado o desvinculado y el personal de empresas prestatarias de servicios, que están vinculadas a la Institución.

Dentro de la peligrosidad, este tipo de amenazas son las más peligrosas, porque dependiendo de los niveles de acceso a información que posean, pueden ocasionar efectos muy graves en los servicios y sistemas internos.

En lo que respecta a las amenazas externas, tenemos:

- **Organizaciones cibercriminales y grupos patrocinados por Estados:** Son aquellas organizaciones cibercriminales que cuentan con un gran financiamiento. Las fuentes de ese financiamiento pueden ser de las más variadas, pueden provenir de Estados, como de parte de organizaciones delictivas (narcotráfico) o autofinanciadas por medio de acciones propias. Es un escenario sumamente complejo, en el cual se encuentran vinculados estados, organizaciones criminales, narcoterrorismo, etc. Merece un capítulo aparte. En este apartado están categorizados los grupos APT, o Amenazas Persistentes Avanzadas, como Fancy Bear, de origen ruso, o Lazarus, de Corea del Norte.
- **Grupos Hacktivistas:** Otro actor de amenaza externa está representado por los grupos hacktivistas, que persiguen objetivos políticos, como lo es, por ejemplo, Anonymous. Este grupo se caracteriza por su uso de la máscara de Guy Fawkes y por llevar a cabo acciones y campañas de ciberactivismo en apoyo a causas que consideran justas, a menudo criticando o atacando a gobiernos y corporaciones.
- **"Script Kiddies" y Cibercriminales menores:** Otra amenaza externa está representada por cibercriminales menores, lobos solitarios o "script kiddies". Con esto, nos referimos a individuos u organizaciones muy pequeñas. "Script Kiddies" es el nombre que se le da a los cibercriminales nuevos, aquellos que tienen poco conocimiento técnico y que llevan a cabo ataques sin total conocimiento de las implicancias de sus hechos.
- **Hackers militares y unidades de guerra cibernética**: Finalmente no podemos dejar de hablar de los "Hackers Militares". Obviamente estamos hablando de un elemento organizado a nivel estatal y militar, que actúa bajo marcos de legalidad. Un ejemplo de estos es el de la Unidad 8200, de Israel, a la que se le atribuye la colaboración con la Agencia Nacional de Seguridad de Estados Unidos (NSA) en la modificación del Virus Stuxnet, y a la que se le atribuye participación en el ataque de los Beepers en el Líbano.

Todas ellas son peligrosas, pero en el contexto de la Ciberguerra y de la Guerra Hibrida, las más relevantes son las Unidades de Guerra Cibernética y las Amenazas Persistentes Avanzadas.

U8200: La punta de lanza cibernética israelí.

Un ejemplo de una unidad de Guerra Cibernética es la U8200 israelí. Esta unidad de Inteligencia Militar es considerada como el equivalente a la NSA de Estados Unidos.

La Unidad 8200 es una **unidad de inteligencia militar** de Israel, a menudo considerada el equivalente de la NSA de Estados Unidos, cuyo principal propósito es la recopilación masiva de ciberinteligencia y la ejecución de operaciones ofensivas en el ciberespacio.

La unidad cuenta con un grupo de talentos excepcionalmente grande para el tamaño de Israel, atrayendo entre 1.000 y 2.000 de los mejores talentos del país cada año, y cuyos integrantes son seleccionados desde las etapas educativas más tempranas de modo de contar con personal de excelencia para las acciones de ciberguerra.

La clave de la eficiencia y el renombre que ha ganado esta unidad está en el personal de alta calidad y su rápida rotación, lo que contribuye a cambios rápidos y respuestas ágiles al entorno tecnológico cambiante. Este personal es menos rígido y a menudo impulsa la innovación desde abajo, cambiando de profesión cada década, lo cual refleja una política impulsada por Israel desde hace más de 40 años.

La unidad, junto con la Unidad 81 (la unidad de tecnologías avanzadas), ha funcionado como importantes incubadoras y aceleradoras de startups de alta tecnología en Israel. Muchos líderes de empresas de ciberseguridad como Check Point, Palo Alto Networks y NICE Systems, son veteranos de estas unidades.

Las capacidades cibernéticas ofensivas de Israel permitirían contrarrestar una variada gama de amenazas, entre las que se le atribuyen:

- Neutralizar la amenaza de cohetes avanzados de Hezbolá.
- Inhabilitar aviones enemigos en vísperas de una guerra sin arriesgar vidas humanas.
- Afectar el sector energético de Irán al inicio de un conflicto mayor, lo que tendría un impacto estratégico más amplio que la neutralización táctica de sistemas de armas.

En resumen, la Unidad 8200 es una **unidad de élite con capacidades cibernéticas avanzadas**, reconocida por su rol en la recopilación de inteligencia, operaciones ofensivas y como motor clave de la innovación tecnológica en Israel.

Lazarus: El atacante silencioso norcoreano

Un ejemplo de un APT, es Lazarus. Este grupo es reconocido como una amenaza internacional de las más sofisticadas y prolíficas.

Su historial está marcado por campañas de espionaje cibernético, sabotaje y robos financieros multimillonarios que han sacudido a instituciones y empresas en todo el mundo, los que se sospecha que están siendo destinados al financiamiento del desarrollo de capacidades nucleares norcoreanas.

Como ya se ha mencionado**,** la atribución en el ciberespacio no es una tarea sencilla, pero el consenso general entre la comunidad de inteligencia y las firmas de seguridad apunta directamente a que este grupo está patrocinado por Corea del Norte. Se cree que el Lazarus Group es una parte integral del Reconnaissance General Bureau (RGB), la principal agencia de inteligencia extranjera de Corea del Norte.

El respaldo estatal les proporciona recursos significativos, persistencia y una motivación que trasciende las ganancias económicas individuales. Su objetivo principal parece ser doble: obtener divisas extranjeras para el régimen norcoreano, eludiendo las sanciones internacionales, y llevar a cabo operaciones de espionaje y sabotaje en línea con los intereses estratégicos del país.

Financiación a través del Ciberdelito:

A diferencia de otros grupos APT Lazarus se distingue por su marcado interés en el robo financiero a gran escala. Sus métodos para lograr este objetivo son variados y sofisticados:

- **Ataques a instituciones financieras:** Utilizan malware personalizado y técnicas de movimiento lateral para acceder a sistemas críticos y realizar transferencias fraudulentas de fondos desde instituciones financieras. Un ejemplo de ello fue el robo al Banco de Bangladesh en 2016, donde intentaron sustraer casi mil millones de dólares, y aunque finalmente lograron "solo" 81 millones, es un ejemplo de su capacidad.
- **Robo de criptomonedas:** En los últimos años, con el auge de las criptomonedas, el Lazarus Group ha adaptado sus tácticas para incluir el robo de activos digitales. Se han atribuido a este grupo numerosos ataques a casas de cambio de criptomonedas y billeteras virtuales, resultando en pérdidas multimillonarias.
- **Ransomware:** Aunque menos prominente que sus ataques financieros directos, el Lazarus Group también ha utilizado ransomware como una herramienta para generar ingresos, a menudo combinándolo con otras tácticas como la exfiltración de datos.

Tácticas, Técnicas y Procedimientos (TTPs):

El Lazarus Group se caracteriza por una serie de TTPs distintivas que les permiten llevar a cabo sus complejas operaciones:

- **Ingeniería Social y Spear-Phishing:** Inicialmente, suelen infiltrarse en las redes objetivo a través de correos electrónicos de spear-phishing altamente dirigidos, donde envían archivos adjuntos maliciosos o enlaces a sitios web comprometidos que explotan vulnerabilidades o engañan a los usuarios para que revelen sus credenciales.
- **Explotación de Vulnerabilidades Zero-Day y N-Day:** El grupo tiene la capacidad de identificar y explotar vulnerabilidades de software, tanto aquellas que son desconocidas para el proveedor (zero-day) como aquellas que ya han sido divulgadas, pero aún no parcheadas (N-day).
- **Malware Personalizado:** El Lazarus Group desarrolla y utiliza una amplia gama de malware personalizado y sofisticado. Estas herramientas están diseñadas específicamente para sus objetivos y a menudo incluyen funcionalidades como puertas traseras (backdoors), registradores de pulsaciones de teclas (keyloggers), herramientas de movimiento lateral y mecanismos para la exfiltración de datos. Algunos de sus códigos maliciosos más conocidos incluyen "WannaCry", aunque su atribución directa sigue siendo objeto de debate.
- **Técnicas de Ofuscación y Antianálisis:** Para evitar la detección, el grupo emplea diversas técnicas de ofuscación de código y anti-análisis, dificultando la labor de los investigadores de seguridad. Esto incluye el uso de cifrado personalizado, la inyección de código en procesos legítimos y el uso de herramientas para desactivar software de seguridad.
- **Ataques a la Cadena de Suministro:** En algunos casos, se ha observado al grupo comprometiendo proveedores de software para llegar a sus objetivos finales, lo que demuestra un alto nivel de sofisticación.
- **Uso de Herramientas de Código Abierto y Dual-Use:** Además de su malware personalizado, el grupo también utiliza herramientas de código abierto y software legítimo (dual-use) para llevar a cabo sus ataques, lo que dificulta aún más su detección y atribución.
- **Ataques Destructivos:** En ciertas ocasiones, especialmente en operaciones de sabotaje, el Lazarus Group ha empleado malware diseñado para borrar discos duros y dejar inutilizables los sistemas comprometidos.

Casos Notorios:

El Lazarus Group ha estado implicado en una serie de incidentes de ciberseguridad de alto perfil que han tenido un impacto significativo a nivel global:

- El Ciberataque a Sony Pictures (2014): Este ataque, atribuido al grupo, resultó en la filtración masiva de correos electrónicos, información personal de empleados y películas inéditas. Se cree que la motivación detrás de este ataque fue evitar que la película "The Interview", una sátira política sobre el líder norcoreano Kim Jong-Un, fuera estrenada. El ataque incluyó la destrucción de gran parte de la infraestructura informática de Sony Pictures.

- El Robo al Banco de Bangladesh (2016): Como se mencionó anteriormente, este intento de robo de casi mil millones de dólares a través de la red SWIFT puso de manifiesto la audacia y la sofisticación de las capacidades financieras del Lazarus Group. A pesar de que una parte de la transferencia fue bloqueada debido a un error tipográfico, los 81 millones de dólares robados causaron un gran revuelo en el mundo financiero.

- El Ataque de Ransomware WannaCry (2017): Si bien la atribución directa sigue siendo debatida, muchas investigaciones apuntan al Lazarus Group como el responsable inicial de la propagación de este ransomware a nivel mundial. WannaCry cifró los archivos de cientos de miles de ordenadores en más de 150 países, afectando a hospitales, empresas y agencias gubernamentales.

- Ataques Continuos a la Industria de Criptomonedas: Desde 2017, el Lazarus Group ha mantenido una campaña constante de ataques contra casas de cambio de criptomonedas y plataformas relacionadas, robando cantidades significativas de activos digitales. Estos ataques han continuado hasta la actualidad, lo que subraya su persistente interés en esta forma de financiación ilícita.

Estos son dos ejemplos de entidades que operan en el ciberespacio, una de ellas con el aval y reconocimiento del estado, otra de ellas con el patrocinio encubierto. Muchas de las APT tienen características similares a las presentadas en el ejemplo de Lazarus, aunque difieren en las víctimas y alineaciones geopolíticas.

Acciones en el Ciberespacio en los Conflictos Actuales.

A continuación, para cerrar el artículo, vamos a ver algunos ejemplos de ciberataques llevados a cabo contra objetivos ucranianos y europeos, atribuidos a actores patrocinados por Rusia, para comprender las posibilidades que ofrecen las operaciones en el ciberespacio.

- *13-14.01.2022. Ataque masivo a sitios web del gobierno ucraniano. Durante la noche del 13 al 14 de enero, hackers lanzaron un ataque masivo a sitios web del gobierno ucraniano. Esto incluye los sitios web del Ministerio de Educación, el Ministerio de Asuntos Exteriores, el Ministerio de Deportes, el Ministerio de Energía, el Ministerio de Agricultura, el Ministerio de Asuntos de Veteranos, el Ministerio de Medio Ambiente, el Servicio Estatal de Emergencias y el Tesoro. Los atacantes comprometieron la infraestructura de una empresa comercial que tenía acceso administrativo a los sitios web afectados, lo que les permitió llevar a cabo el ataque.*

- *26.01.2022. Ciberataque al sitio web Ukraine.ua. Durante la noche del 26 de enero, se lanzó un ciberataque al sitio web oficial de Ucrania, Ukraine.ua. Como resultado del ataque, el sitio web estuvo inaccesible para los usuarios durante varias horas. A las 13:00 del 26 de enero de 2022, se restableció el acceso al sitio web. Ukraine.ua se lanzó el 14 de enero de 2021 y sirve como portal para el público extranjero sobre la auténtica Ucrania moderna:*

un país creativo, dinámico e innovador, diverso y con una naturaleza encantadora, un país de libertad y dignidad, donde milenios de historia y cultura se complementan con una ambiciosa visión de futuro.

- *15/02/2022 Ciberataques a bancos y sitios web del Ministerio de Defensa. En la noche del 13 al 14 de enero, los sitios web del gobierno ucraniano fueron objeto de un ciberataque masivo. En concreto, los sitios web del Ministerio de Educación, el Ministerio de Asuntos Exteriores, el Ministerio de Deportes, el Ministerio de Energía, el Ministerio de Política Agraria, el Ministerio de Asuntos de Veteranos, el Ministerio de Ecología, el Servicio Estatal de Emergencias y el Tesoro Estatal fueron atacados.*

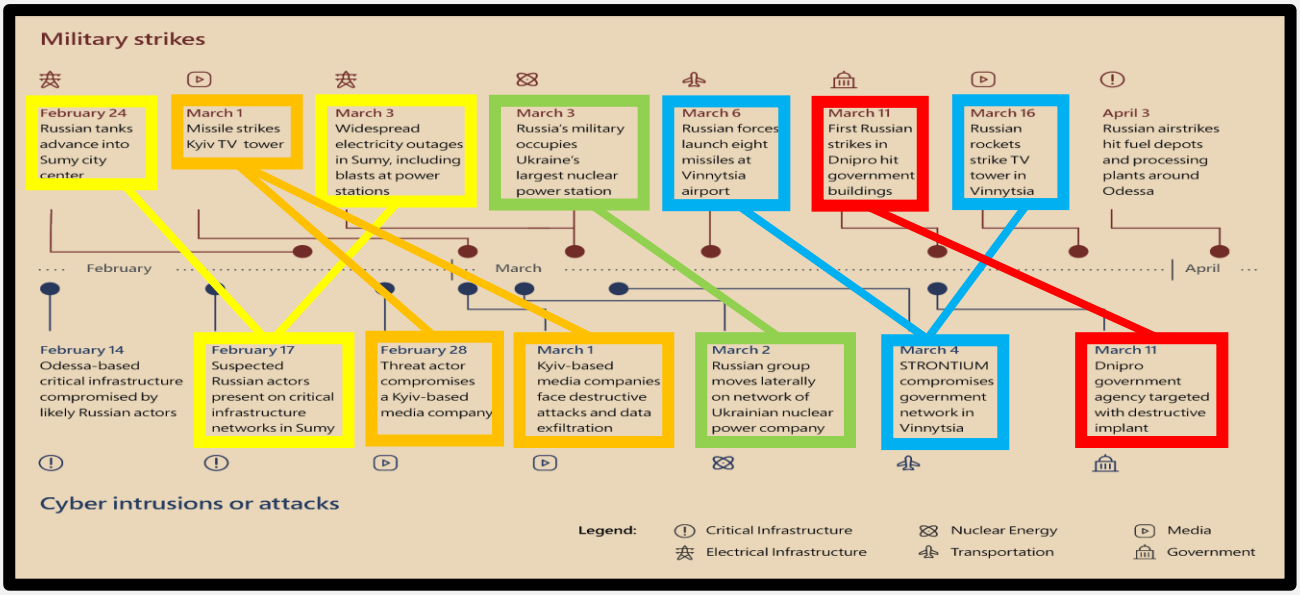
- *El 23/02/2022, una nueva serie de ataques DDoS masivos tuvo como objetivo los sitios web de instituciones gubernamentales y bancarias. Algunos de los sistemas de información atacados quedaron inaccesibles o su funcionamiento fue interrumpido, lo que obligó a desviar el tráfico para minimizar los daños. Sin embargo, otros sitios resistieron eficazmente los ataques y funcionaron con normalidad.*

- *El 24 de febrero, las tropas rusas iniciaron una invasión a gran escala de Ucrania, acompañada de ataques con misiles contra instalaciones civiles y militares.*

Ese mismo día, un ciberataque a gran escala interrumpió el acceso a internet por satélite. Los hackers desactivaron los módems que se comunican con el satélite Viasat KA-SAT, que proporciona acceso a internet a clientes en Europa, incluida Ucrania. Rusia utiliza los ciberataques para debilitar a Ucrania y su capacidad para contrarrestar eficazmente las agresiones convencionales.

- *En abril de 2022 actores pro-rusos llevaron a cabo Ciberataques a tres empresas europeas de energía eólica. Los hackers intentaron sembrar el caos en un sector que beneficiará a Ucrania y reducirá su dependencia del petróleo y el gas rusos. Según Deutsche Windtechnik AG, los sistemas de control remoto de aproximadamente 2000 aerogeneradores en Alemania se vieron afectados, y las conexiones de monitorización remota de datos se restablecieron en uno o dos días. El servicio de atención al cliente se reanudó el 14 de abril (tres días después del ataque) y funcionó con pocas restricciones.*

Desde el inicio de la invasión rusa de Ucrania el 24 de febrero, además, un informe de lecciones aprendidas de la OTAN, del año 2022, permitió observar que grupos rusos de ciberamenazas realizaron acc iones para apoyar los objetivos estratégicos y tácticos de las fuerzas armadas rusas.



Una cronología de ataques militares e intrusiones cibernéticas muestra varios ejemplos de operaciones de redes informáticas y operaciones militares que parecen funcionar en conjunto contra un objetivo común, y aunque no está claro si existe coordinación o una asignación centralizada de tareas, la relación entre las acciones en el ciberespacio, y las acciones cinéticas que se dieron luego, fueron evidentes.

La gran mayoría de las operaciones cibernéticas llevadas a cabo contra Ucrania en el contexto de la guerra, estuvieron dirigidas a degradar, perturbar o desacreditar las funciones gubernamentales, militares y económicas de Ucrania, asegurar el acceso a infraestructuras críticas y reducir el acceso del público ucraniano a la información.

Por otra parte, en el transcurso del conflicto proliferaron grupos hacktivistas que llevaron a cabo operaciones cibernéticas en su nombre. Estos grupos pueden tener diversos grados de afiliación con las agencias de inteligencia o entidades gubernamentales rusas. A menudo participan en campañas de desinformación, propagan propaganda y lanzan ciberataques contra oponentes políticos y otros países.

Vale mencionar, nuevamente, que atribuir acciones en el ámbito cibernético puede ser difícil, y que las responsabilidades y afiliaciones específicas de las distintas unidades cibernéticas pueden no ser siempre transparentes. Dado que el panorama de la ciberguerra está en constante evolución, es crucial adaptar continuamente las capacidades cibernéticas y estructuras organizativas para responder a las amenazas y desafíos emergentes.

Conclusiones

A lo largo de este artículo hemos caracterizado al ciberespacio, hemos visto su importancia en las operaciones militares y estatales, lo que nos llevó a la definición de la ciberguerra y su relación con las guerras híbridas.

Todo lo mencionado anteriormente, es posible ya que el ciberespacio es un escenario relativamente moderno, en el cual diferentes actores, desde muy sofisticados, hasta individuos con pocos conocimientos, pueden llevar a cabo acciones de gran escala contra infraestructuras o sistemas sofisticados, ocasionando desde desestabilización hasta pérdidas económicas y reputacionales. Estas posibilidades no son desaprovechadas por los países que, empujados por sus intereses geopolíticos, llevan a cabo diferentes tipos de acciones en el ciberespacio, con relativa seguridad de que no se podrá determinar su responsabilidad en los hechos.

Como ya se ha mencionado muchas veces, la dificultad en la atribución de un ciberataque, la posibilidad de anonimato en la red, y el riesgo de exponerse a grandes sanciones económicas, transforman al ciberespacio en un escenario ideal para operaciones de ciberespionaje y cibersabotajes, permitiendo la operación en una zona gris no definida y sobre la que no hay consenso para la definición de un acto bélico.

Por otra parte, el alcance global del ciberespacio y la imposibilidad de determinar cuales son las "fronteras" en el mismo, conlleva grandes desafíos para los países, dado que se dificulta definir la superficie a defender.

Finalmente, es importante destacar el ejemplo israelí en lo referido a la capacitación y selección de personal para la conformación de una unidad especializada. Este proceso debe ser encarado por la Institución con mucha mayor preocupación, dando relevancia al ciberespacio como un dominio operativo, el cual es necesario comprender de forma específica y en su relación con los demás dominios operativos (tierra, mar y aire), y como tal una función de Comando. Esto hace necesaria la incorporación de más capacitaciones, currículas de estudio que incorporen a la

ciberdefensa como una materia y un adecuado seguimiento profesional para la identificación del personal más capacitado para desarrollarse en esta función específica dentro de la Institución.

Bibliografía.

- *"Cyber Warfare Conflict Analysis and Case Studies"*, Mohan B. Gazula (2017).
- *"CYBERSPACE OPERATIONS"*, Air Force Doctrine Document (2010).
- "*Encyclopedia of Cyber Warfare*", Paul J. Springer (2017).
- *"La Ciberguerra: sus impactos y desafíos"*, Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile -CEEAG (2017).
- *"Operaciones Militares Cibernéticas"*, E. Vergara, G. Trama *(2016)*
- *"Ciberguerra: tipos, armas, objetivos y ejemplos de la guerra tecnológica."*, Lisa Institute.
- *"Estrategia de Ciberseguridad Nacional"*, Reino de España.
- *"Defense Primer: Cyberspace Operations"*, Departamento de Defensa de EEUU (2023)
- *"Ciberestrategia Nacional 2022"*, Reino Unido (2022).
- *"Estrategia Nacional de Ciberseguridad de la República Argentina"*, Poder Ejecutivo Nacional (2023).
- *"La lógica de la ciberguerra y su relación compleja con la disuasión"*, R. Villagra.
- *"Lazarus Group: La Amenaza Persistente Detrás del Telón de Acero"*, Martín Guerra (2025).
- *"RUSSIAN WAR AGAINST UKRAINE LESSONS LEARNED"*, OTAN (2022)

.

» Operaciones ofensivas en el Ciberespacio. Una visión doctrinal

Por TN Lic. Maximiliano Daniel Gamboa[20]

Introducción

El ciberespacio se ha consolidado como un dominio operativo estratégico que ha alterado la manera en que se planifican y conducen las operaciones militares. Las acciones ofensivas en ese ámbito, orientadas a degradar, interrumpir o destruir sistemas e infraestructuras digitales adversarias, exigen un conocimiento profundo sobre las amenazas, las técnicas de ataque y la manera de articularlas con la lógica doctrinaria convencional. Este artículo plantea un enfoque estructurado desde las perspectivas técnica y militar, proponiendo al modelo Cyber Kill Chain como marco metodológico central y examinando su vinculación con los conceptos y principios propios de las operaciones ofensivas tradicionales, considerando la doctrina de la Armada Argentina.

Como dominio operacional paralelamente a los espacios terrestre, marítimo, aéreo y espacial, el ciberespacio presenta rasgos singulares que obligan a adaptar el pensamiento militar. Sin embargo, pese a esas particularidades, varios postulados clásicos —los "Principios de la Guerra"— siguen siendo aplicables a las operaciones en el ciberespacio, aunque otros principios no encajen exactamente en su sentido estricto.

Operaciones ofensivas en el ciberespacio

Las operaciones ofensivas en el ciberespacio se definen como acciones dirigidas a interferir, degradar, denegar o destruir sistemas de información enemigos[21]. Su objetivo es producir efectos

[20] Teniente de Navío. Licenciado en Recursos Navales para la Defensa.
[21] Evaristo Guevara, "Operaciones Militares Cibernéticas".

militares decisivos mediante medios digitales, a menudo sincronizados con otras dimensiones del conflicto (operaciones conjuntas o combinadas) para alcanzar los objetivos militares[22] asignados.

A diferencia de las acciones defensivas o de respuesta, estas operaciones parten de un análisis deliberado del adversario y una planificación ofensiva centrada en objetivos definidos. Estos pueden incluir, entre otros:

- Interrupción del flujo de información enemigo.
- Sabotaje de infraestructuras críticas de mando y control.
- Desinformación y manipulación cognitiva.
- Destruir físicamente la información del adversario o reducir la efectividad de sus sistemas de comunicación y recolección de información.
- Ataques sobre sistemas logísticos o industriales (ICS/SCADA).

La lógica que rige estas operaciones mantiene estrecha relación con los principios clásicos de la guerra, particularmente los postulados de la guerra de maniobras, la sorpresa, la economía de medios y el esfuerzo principal, como veremos más adelante.

No obstante, como se mencionó anteriormente, las acciones ofensivas están dirigidas a los sistemas de información enemigos, pero ¿qué entendemos por sistema de información?

Sistemas de Información.

Un sistema de información es un conjunto organizado de componentes que trabajan juntos para recopilar, procesar, almacenar y distribuir información con el fin de apoyar las operaciones, la gestión y la toma de decisiones de una organización (Figura N°1). Permite que una información, o dato, que ingresa al sistema, sea procesado y representado en forma que pueda ser interpretada por una persona o componente interno del sistema. El ingreso de datos puede provenir de celulares, computadoras, sensores, etc., los cuales pueden ser representados visualmente por medio de interfaces de usuario. Ejemplos de Sistemas de Información son los Sistemas de Información Geográfico, como QGIS o ArcGIS, o los Sistemas de Gestión de la Información Táctica como el TAK y sus diferentes versiones, o incluso "Pollux[23]" o SITEA[24].

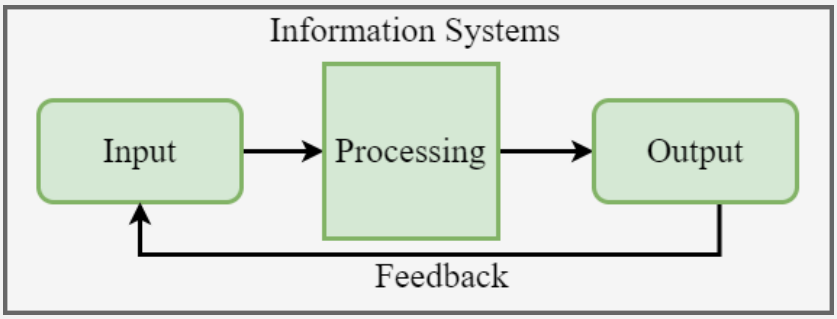


Figura N°1: Esquema de bloques de un Sistema de Información.

[22] Objetivo Militar: Aquel objeto cuya destrucción total o parcial, captura o neutralización ofrece una ventaja militar directa y concreta. Doctrina EMCO.
[23] "Pollux" es un sistema de Comando y Control, y procesamiento de información, desarrollado por la Armada Argentina para las operaciones navales.
[24] "SITEA" Sistema Integrado Táctico de Comando y Control del Ejército Argentino, es un sistema C4ISR (Comando, Comunicaciones, Control, Computación, Inteligencia, Vigilancia y Reconocimiento) desarrollado por el Ejército Argentino.

Es importante, a la hora de planificar un ataque, conocer las partes componentes de un Sistema de Información, dado que esto nos permitirá identificar el, o los, vectores de ataque para ingresar al sistema. Estas partes son:

- Hardware: Conjunto de dispositivos físicos y tangibles, como computadoras, servidores, discos duros, sensores y periféricos, que permiten el procesamiento, almacenamiento y transmisión de la información dentro del sistema.
- Software: Programas y aplicaciones que controlan y coordinan el funcionamiento del hardware y permiten ejecutar tareas específicas, desde sistemas operativos hasta herramientas de gestión y análisis.
- Datos: Conjuntos de hechos, cifras u observaciones sin procesar que, al ser organizados y analizados, se convierten en información útil para la toma de decisiones.
- Procesos: Conjunto de actividades y reglas organizadas que transforman los datos en información significativa, garantizando que el sistema funcione de manera coherente y eficiente.
- Redes: Infraestructura de comunicación que conecta los distintos dispositivos y sistemas, permitiendo el intercambio y acceso a datos e información en forma local o remota.
- Bases de Datos: Sistemas estructurados de almacenamiento que organizan, resguardan y permiten el acceso eficiente a grandes volúmenes de datos de forma segura y coherente.
- Operadores (personas): Usuarios y responsables que interactúan con el sistema, ya sea ingresando datos, interpretando resultados o supervisando los procesos, y que aportan criterio, juicio y control a su funcionamiento.

De acuerdo con las partes identificadas, como componentes de un sistema de información, un atacante puede buscar realizar diferentes tipos de ataques. Este cuadro resume alguno de ellos (Figura N°2).

Componente	Vulnerabilidades clave	Tipos de Ataques
Hardware	Fallas físicas, firmware, accesos físicos	Meltdown, Spectre, Rowhammer, DMA
Software	Errores de código, dependencias	RCE, buffer overflow, backdoors
Datos	Falta de cifrado, accesos sin control	Ransomware, exfiltración, data breach
Procesos	Políticas débiles, falta de control	Ingeniería social, sabotaje interno
Redes	Puertos abiertos, protocolos inseguros	MITM, DDoS, spoofing, sniffing
Bases de Datos	Contraseñas débiles, SQL sin sanitizar	SQLi, robo, corrupción de datos

Figura N°2: Tipos de ataques a componentes de un Sistema de Información

La guerra en curso entre Rusia y Ucrania ha dejado numerosos ejemplos de este tipo de acciones (Figura N°3).

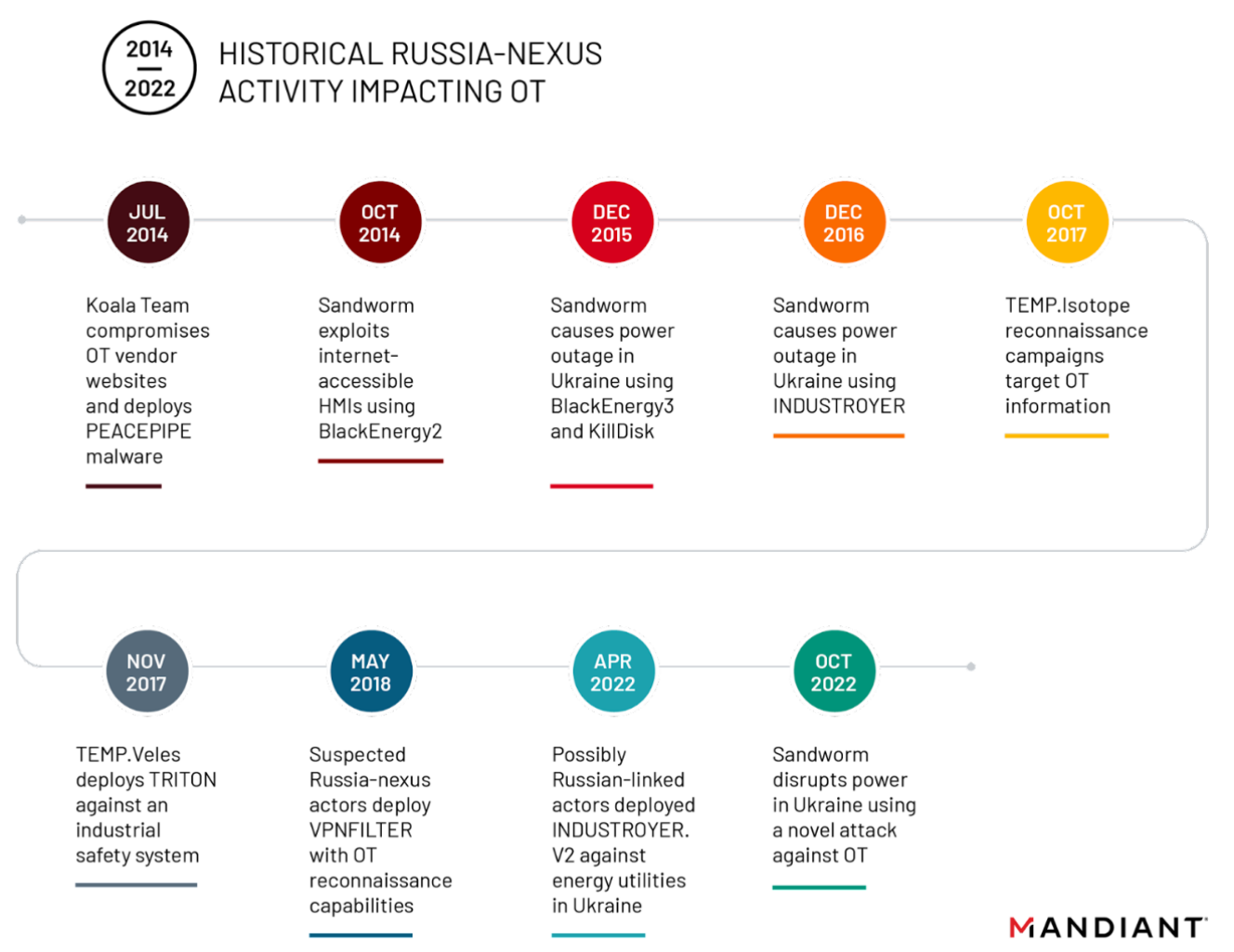


Figura N°3: Actividad de Rusia contra infraestructuras OT de Ucrania.

Fuente: *Mandiant Threat Intelligence*

3. La metodología de ataque en el Ciberespacio: La Cyber Kill Chain

Este marco de trabajo (Framework) consiste en una secuencia de pasos ordenados para llevar a cabo un ciberataque. Esta metodología fue desarrollada en mayor detalle en un artículo anterior en esta misma publicación, por lo que a continuación se hará una breve descripción.

Antes de continuar, es importante destacar lo siguiente: No se trata de una secuencia de pasos mandatoria, ni siquiera una sobre la cual haya consenso a nivel internacional, sino que, se trata de una metodología más para comprender como llevan a cabo los ciberataques, los actores mencionados anteriormente.

La cyber kill chain surge del análisis de los ciberataques llevados a cabo contra organizaciones e instituciones, y a partir de allí se identificaron los patrones de ataque que permitieron desarrollar, o concluir, que los pasos para un ciberataque exitoso.

Este modelo constituye una herramienta doctrinal útil para comprender y estructurar ataques cibernéticos avanzados. Divide el proceso en siete etapas secuenciales (Figura N° 4):

- Reconocimiento: identificación de blancos, recopilación de información técnica, humana y organizacional. Incluye OSINT, escaneos de red, análisis de puertos y servicios.

Lo que se busca en esta etapa es identificar **la superficie de ataque** del enemigo, y con esto nos referimos a aquello servicios, softwares, personas, etc., que nos puedan servir como vector de ingreso al sistema para llevar a cabo nuestro cometido.

- **Preparación (Weaponization)**: Una vez identificada la superficie de ataque se lleva a cabo la Preparación o Armamentización. En muchos lados van a encontrarla con el segundo término.

En esta etapa, el atacante adquiere o desarrolla las herramientas y exploits[25] necesarios para llevar a cabo el ataque. Esto implica la búsqueda de vulnerabilidades conocidas o la creación de malware personalizado para aprovechar las debilidades identificadas durante la fase de reconocimiento.

- **Entrega**: Aquí, el atacante proporciona el medio para entregar el ataque al objetivo. Esto puede implicar el envío de correos electrónicos de phishing, la explotación de vulnerabilidades en servicios web, la inserción de dispositivos USB maliciosos o cualquier otra técnica para engañar al objetivo y lograr que ejecute el ataque. En esta etapa se determina el payload[26] (o carga activa del exploit) que cumplirá el objetivo del ciberataque.
- **Explotación**: En esta etapa, el atacante busca explotar las vulnerabilidades en el sistema objetivo. Puede incluir la ejecución de código malicioso, la explotación de vulnerabilidades de software o hardware, la manipulación de archivos o la realización de acciones que permitan al atacante ganar control sobre el sistema.
- **Instalación**: Después de obtener acceso al sistema, el atacante busca establecer una presencia persistente para mantener el control incluso después de que se detecte y elimine el acceso inicial. Esto puede implicar la instalación de puertas traseras, la creación de cuentas de usuario adicionales o la modificación de configuraciones para facilitar el acceso futuro.
- **Comando y Control (C2):** En esta etapa, el atacante establece una comunicación encubierta con los sistemas comprometidos. Esto permite al atacante mantener el control y enviar instrucciones adicionales. Puede usar canales cifrados, DNS tunneling[27] o servidores remotos (C2 servers).

Generalmente, como veremos más adelante, un atacante establece servidores propios, o bajo su control, para llevar a cabo la exfiltración de información, o la comunicación con los sistemas, para dificultar la trazabilidad y facilitar el anonimato. Esta es una de las grandes problemáticas para la atribución de un ciberataque.

- **Acciones sobre el objetivo**: En la última etapa del Modelo Cyber Kill Chain, el atacante lleva a cabo la acción final para lograr sus objetivos específicos. Esto puede incluir actividades como la exfiltración de datos confidenciales, el sabotaje de sistemas, el robo de información valiosa o cualquier otro objetivo que el atacante haya buscado desde el principio.

[25] Exploit: Un "exploit" en seguridad informática es una técnica o código que se aprovecha de una vulnerabilidad en un software, aplicación, sistema operativo o hardware para obtener acceso no autorizado o realizar acciones no permitidas. Los exploits pueden ser utilizados para instalar malware, robar datos, o tomar control del sistema.

[26] Payload: En ciberseguridad, un "payload" se refiere a la parte de un programa malicioso (malware) que realiza la acción dañina específica en un sistema, como borrar archivos, robar datos o tomar el control del equipo. Es la carga útil, la parte del ataque que causa el daño real.

[27] La tunelización DNS es una técnica utilizada por atacantes para ocultar tráfico malicioso dentro de consultas y respuestas DNS, permitiendo la transferencia de datos y el control de sistemas comprometidos a través de redes que generalmente no son supervisadas para este tipo de tráfico.

El conocimiento profundo de esta cadena no solo permite ejecutar ataques más eficientemente, sino también identificar puntos de detección temprana y contención para fines defensivos.

Figura N°4: Modelo de Cyber Kill Chain.

4. Aplicación de Conceptos de las Operaciones Ofensivas

Finalmente, este último apartado quiero dedicarlo a establecer las relaciones entre los conceptos asociados tradicionalmente a las operaciones ofensivas, tales como principios, fases y conceptos de la Guerra de Maniobras, y cómo estos se traducen (o no) a las operaciones en el ciberespacio.

Vale mencionar, antes de iniciar con el análisis, que muchos de los conceptos de las operaciones tradicionales, están muy vinculados al terreno y a las acciones cinéticas por parte de elementos de maniobra con poder de fuego o poder de incidencia sobre un enemigo físico tradicional. Si bien el ámbito de aplicación de la Armada Argentina es el marítimo, este análisis estará centrado en las características de las operaciones ofensivas a desarrollarse en ambientes anfibios o terrestres, dado que la naturaleza marítima implicaría otras consideraciones para la planificación de operaciones navales ofensivas tradicionales.

Para este análisis tomé como conceptos, los principios de la guerra vertidos en la Doctrina Fundamental de la Armada Argentina (DOCFUARA) y los principios vertidos en la reglamentación del Ejército Argentino, que se condicen, en muchos, con los principios presentes en la Doctrina Militar Conjunta.

Habiendo hechos las aclaraciones pertinentes, a continuación, desarrollaré el paralelismo entre las dos fuentes reglamentarias y las conclusiones a las que he arribado.

4.1 Relación entre los Principios de la Guerra y su aplicación a las Operaciones Ofensivas en el Ciberespacio.

Objetivo: Hay quienes dicen que las operaciones en el ciberespacio no tienen un objetivo, o no se debería aplicar este principio ya que no están orientadas al objetivo decisivo y que el afán de los militares por tener objetivos claros, definidos y decisivos, limitan las opciones de accionar del decisor estratégico[28]. Disiento en ello, dado que no todos los objetivos son decisivos, y está claro que las operaciones en el ciberespacio se deben llevar a cabo con un objetivo claro, que tiene que estar concatenado con los objetivos de otros elementos. Tal y como lo expresa Guevara en el libro

[28] Robert Leonhard, "The Principles of War for the Information Age".

"Operaciones Militares Cibernéticas", ¿cómo podrían saber los comandantes subordinados cuándo se han alcanzado los criterios de terminación?"

Habiendo hecho esta observación, destaco lo siguiente:

EA	ARA	Definición	¿Aplica?
Objetivo	**Objetivo**	Dirigir cada operación militar hacia un objetivo claro, definido, decisivo y alcanzable	**En las operaciones en el ciberespacio, se planifican acciones contra objetivos materiales concretos, o inmateriales, como lo es el caso de las operaciones de ciberinfluencia.**

Unidad de Comando/Control: Es el principio o axioma que consiste en el ejercicio de la conducción bajo un asolo comando responsable, a efectos de asegurar la unidad de esfuerzo, la economía de medios y la coordinación en el efectivo cumplimiento de la misión asignada.

EA	ARA	Definición	¿Aplica?
Unidad de Comando	**Control**	Asegurar la unidad de esfuerzo bajo un CTE responsable para cada objetivo	**Existe la figura de un Comandante y un Comando Conjunto, u organización equivalente. En Argentina es el Comando Conjunto de Ciberdefensa.**

Seguridad: El principio de seguridad es aquel cuya adopción permitirá mantener la integridad y aptitud para el combate de las fuerzas propias, en todas las operaciones militares. Bajo esta premisa se deben planificar las operaciones ofensivas en el ciberespacio para lograr los objetivos planificados, manteniendo la integridad de los medios y personal responsable de ejecutar tales acciones. Aún los sistemas informáticos más perfectos siguen siendo perfectamente explotables por personas que los utilizan para los propósitos para los que fueran diseñados, pero con resultados y objetivos nefastos.

EA	ARA	Definición	¿Aplica?
Seguridad	**Seguridad**	Evitar o impedir que el enemigo adquiera una ventaja inesperada o sorpresiva.	**En las operaciones en el ciberespacio, se aplican diferentes medidas de seguridad que permitan llevar a cabo las operaciones en anonimato, lo cuál es una condición necesaria para lograr la persistencia, la no atribución y poder explotar el éxito de un ciberataque.**

Iniciativa: Es un principio que el EA lo tiene como parte del Principio de la Ofensiva, y reconocido por la Marina como un principio por su importancia y transversalidad a todo tipo de operación, como una condición inherente para alcanzar el éxito. En otras palabras, es la facultad de gobernar el orden de los acontecimientos en los términos que interesen a la acción propia, además, permite a las organizaciones operativas estar dispuestas para actuar de forma proactiva y mantener de una manera constante la presión sobre el adversario, adelantándose a sus acciones y decisiones.

EA	ARA	Definición	¿Aplica?
	Iniciativa	Capacidad para tomar la ofensiva y obligar al enemigo a reaccionar a sus movimientos.	**El manteniemiendo de la iniciativa se logra por medio de la persistencia. Generalmente, cuando una organización descubre un ciberataque, la primer medida que toma es la contención, para evitar la propagación, sobre todo en el caso de malwares. La posibilidad de adaptarse a los cambios, o a las estrategias defensivas de un enemigo, estará dado por el control que un atacante haya ganado en su cadena de muerte, por la capacidad técnica de sus operadores y por la información que se tenga de la organización enemiga. Para ello toma vital relevancia el reconocimiento (que es permanente)**

Libertad de Acción: Es la posibilidad de decidir, preparar y ejecutar los planes a pesar de la voluntad del adversario. El mando procurará conservarla a todo trance y, si la pierde, tratará de recuperarla

lo antes posible. Requiere capacidad de conocer al adversario, el entorno y los medios propios. El arte militar consiste fundamentalmente en la lucha por alcanzarla.

En las operaciones en el ciberespacio aplica el principio de la libertad de acción. Se obtiene en el momento en el que el atacante es capaz de llevar a cabo modificaciones en los sistemas, que le permitan mantenerse sin ser descubierto dentro de los mismos.

EA	ARA	Definición	¿Aplica?
Libertad de Acción		Disponer de una situación militar favorable que permita la aplicación del poder de combate libre de obstáculos (ENO + AROP) y/ o servidumbres (internas).	**Aplica en el momento en que se lleva a cabo la instalación y el comando y control.**

Masa: En mi apreciación no aplica en las operaciones en el ciberespacio, por lo mencionado debajo. Mi punto de vista difiere con el de otros autores, como Evaristo Guevara, autor de "Operaciones Militares Cibernéticas". En su libro menciona que el principio de masa se cumple por que un ciberataque confluye junto a otros esfuerzos llevados a cabo en otros dominios, en lo cual estoy de acuerdo, aunque él no menciona el caso de un ciberataque por sí solo. En el nivel operacional, que es el nivel para el que está escrita la bibliografía, es algo comprensible y visible el principio de masa, no así para un ciberataque llevado a cabo en forma aislada de otras acciones cinéticas, que es el caso de la interpretación.

En opinión de este autor, el principio de masa hace alusión a la concentración de poder de combate en un lugar adecuado, de lo que se deriva una pregunta, que incluso el mismo autor se hace luego, *"¿dónde comienza y termina el espacio cibernético para el Comandante Operacional?, ¿cómo puede diferenciarse una virtual ciberzona de operaciones conjunta de los dominios de tierra, mar y aire definidos por límites geográficos?"*, y la respuesta es que el ciberespacio no tiene limitaciones geográficas, tiene componentes e infraestructuras que pueden ser referenciadas geográficamente, pero no están centralizadas. Un ejemplo de esto es la nube, la cual está compuesta por una infraestructura distribuida a nivel global, lo que hace impracticable la concentración de poder de combate en un solo lugar, ya que los data-centers de los proveedores de servicio están dispersos.

La imposibilidad de definir límites geográficos precisos en el ciberespacio dificulta aplicar el principio de masa en su forma tradicional. En ausencia de un "lugar" donde concentrar fuerzas, el poder de combate no se acumula físicamente, sino que se dispersa y se sincroniza para generar efectos en nodos o sistemas distribuidos.

EA	ARA	Definición	¿Aplica?
Masa	**Concentración**	Concentrar los efectos del poder de combate, en el lugar y tiempo más ventajoso para producir resultados decisivos (tiene a la Economía de Esfuerzo como corolario)	**No aplica. En las operaciones en el ciberespacio no existe la posibilidad de concentrar efectos de ciberarmas en un lugar y tiempo más ventajoso. Se busca el máximo efecto en un momento indicado, pero sin concentración.**

Sorpresa: Consiste en obligar al adversario a actuar en el lugar, en las condiciones o en el momento para él inesperados, o en emplear medios o procedimientos por él desconocidos, para situarlo en condiciones de inferioridad y conseguir con ello efectos mayores con el mismo esfuerzo o que serían difícilmente alcanzables por otros medios.

EA	ARA	Definición	¿Aplica?
Sorpresa	**Sorpresa**	Su propósito es accionar sobre el oponente en un lugar y momento o en una forma tal, para la cual no se encuentre preparado.	**Aplica en los términos enunciados. Es el factor que se busca obtener mediante diferentes tipos de acciones previas y en el sistema enemigo para obtener ventaja de la persistencia e instalación o modificaciones al Sistema enemigo.**

Ofensiva: Diferentes autores hablan de la ofensiva en los mismos términos que en la definición mostrada debajo. Si al principio lo aplicamos a las acciones ofensivas en el ciberespacio, es verdad que se puede hablar de mantener, retener, recuperar, explotar la iniciativa, aunque se logra conjugando diferentes acciones. No es el término en el que está explicado en el cuadro, no obstante, podemos hablar de ataques como DDos, SQLI, exfiltración de datos, encriptación de datos, etc., pero cada ataque tiene su propia cadena de muerte, y como proceso único entiendo que se pierde parcialmente la iniciativa una vez se ha descubierto el ataque.

EA	ARA	Definición	¿Aplica?
Ofensiva	**Ofensiva**	Tomar, retener y explotar la iniciativa.	**La iniciativa no se pierde totalmente, y el mantenieminto de la misma dependerá de las medidas de persistencia que se hayan establecido durante el tiempo de permanencia en la red (sin ser detectado).**

Maniobra: En lo que respecta a la maniobra, entiendo que no aplica en los términos enunciados, ya que es un principio muy ligado al posicionamiento de tropas en el terreno, lo cual no quiere decir que no haya "movimiento" dentro de una red. En las operaciones en el ciberespacio se habla de CIBERMANIOBRA. La cibermaniobra es la aplicación de la fuerza para capturar, interrumpir, negar, degradar, destruir o manipular sistemas de cómputos y recursos de información con el fin de lograr una posición ventajosa respecto a sus competidores. No obstante, la maniobra se da en términos de protocolos, código y mediante la modificación del punto de ataque.

EA	ARA	Definición	¿Aplica?
Maniobra		Colocar al oponente en una posición de desventaja por medio de la aplicación flexible del poder de combate.	**No aplica en los términos enunciados. Existen técnicas de movimiento lateral y escalamiento en las redes enemigas, pero son para la detección de vulnerabilidades, no para colocar al enemigo en una posición desventajosa.**

Movilidad: En lo que respecta al principio de la movilidad, no aplica en los términos enunciados, de hecho, el Principio de movilidad no está contemplado en ninguna doctrina. Cómo lo utiliza la Armada, en todo el resto del mundo, se utiliza el término "Maniobra". Para el caso de las operaciones en el ciberespacio es exactamente lo mismo.

EA	ARA	Definición	¿Aplica?
Maniobra		Colocar al oponente en una posición de desventaja por medio de la aplicación flexible del poder de combate.	**No aplica en los términos enunciados. No obstante, existe un concepto llamado "cibermaniobra", que es la aplicación de la fuerza para capturar, interrumpir, negar, degradar, destruir o manipular sistemas de cómputos y recursos de información con el fin de lograr una posición ventajosa respecto a sus competidores.**
	Movilidad	"Versión superadora" de la Maniobra. Contempla los movimientos de fuerzas que hacen posible adquirir la posición	

Simplicidad: Preparación de planes claros y sin complicaciones y órdenes concisas para garantizar una comprensión completa. Todo en la guerra es muy simple, pero lo simple es difícil. La

simplicidad contribuye al éxito de las operaciones. Los planes simples y las órdenes claras y concisas minimizan los malentendidos y la confusión.

EA	ARA	Definición	¿Aplica?
Simplicidad	**Simplicidad**	Preparar planes claros y con ordenes concisas que aseguren su comprensión.	**Se dan lineamientos, restricciones, propósitos. Son complejos, técnicamente hablando, y poco detallados.**

Sostenimiento: Es el conjunto de actividades logísticas encaminadas a proporcionar a una fuerza los medios, recursos y servicios necesarios que le permitan mantener la capacidad operativa requerida para el cumplimiento de la misión.

EA	ARA	Definición	¿Aplica?
Sostenimiento		Sostener a las fuerzas propias durante cada maniobra y fase de la campaña, hasta obtener los objetivos operacionales y el EFD.	**Aplica en los términos enunciados.**

Voluntad de vencer: Es el firme propósito del mando y de las tropas de imponerse al adversario y cumplir la misión en cualquier situación por desfavorable que ésta sea. Implica fe en el triunfo, tenacidad para alcanzarlo y actividad insuperable en la ejecución. Se basa en los valores morales que constituyen el primordial exponente de la valía de una fuerza militar.

EA	ARA	Definición	¿Aplica?
Voluntad de Vencer	**Moral**	Consiste en la disposición para empeñar todos los recursos disponibles en la búsqueda del éxito.	**Aplica en los términos enunciados.**

Economía de Fuerzas: Consiste en emplear todo el poder de combate disponible de la manera más efectiva posible; asignar el poder de combate esencial mínimo a los esfuerzos secundarios. La economía de la fuerza es el empleo y la distribución juiciosos de las fuerzas. Ninguna parte de la fuerza debe quedar nunca sin propósito. La asignación del poder de combate disponible para tareas tales como ataques limitados, defensa, demoras, engaños o incluso operaciones retrógradas se mide para lograr masa en otros lugares en el punto y momento decisivos del campo de batalla.

EA	ARA	Definición	¿Aplica?
Economía de Fuerzas	**Economía**	Consiste en dosificar cuidadosamente el poder de combate disponible, de modo de asegurar los medios suficientes en el lugar decisivo, y los mínimos necesarios en las áreas de esfuerzos secundarios.	**Aplica en cuanto a asegurar los medios suficientes en el lugar decisivo, no tanto así en cuanto a la dosificación. Se buscará priorizar la sorpresa por sobre la dosificación de medios.**

Alistamiento: Define la capacidad operativa y la disponibilidad de una unidad para llevar a cabo una determinada misión en una intensidad de entorno establecida.

EA	ARA	Definición	¿Aplica?
	Alistamiento	Organización, adiestramiento, adoctrinamiento y equipamiento de todos los elementos esenciales para hacer la guerra.	**Aplica en los términos enunciados.**

4.2 Relación entre los Principios de la Ofensiva y las Operaciones Ofensivas en el Ciberespacio.

Relacionando los principios de la ofensiva, representa una tarea mucho más difícil relacionar aquellos principios que están íntimamente ligados al terreno, como lo es la conquista de Rasgos Críticos, aun así, he podido trazar el siguiente paralelismo.

PRINCIPIOS DE LA OFENSIVA	¿CUMPLE?
OBTENER Y MANTENER EL CONTACTO	DESDE LA ENTREGA HASTA LA MITIGACIÓN
ACLARAR LA SITUACIÓN	RECONOCIMIENTO
EXPLOTAR LA DEBILIDAD DEL ENEMIGO	EXPLOTACIÓN
CONQUISTAR Y CONTROLAR RRCC	INSTALACIÓN
RETENER LA INICIATIVA	COMANDO Y CONTROL
NEUTRALIZAR LA CAPACIDAD DE REACCIÓN DEL ENEMIGO	INSTALACIÓN - COMANDO Y CONTROL
AVANZAR POR EL FUEGO Y LA MANIOBRA	EXPLOTACIÓN - INSTALACIÓN
MANTENER EL IMPULSO DEL ATAQUE	COMANDO Y CONTROL - ACCIONES EN EL OBJETIVO
CONCENTRAR UN PODER DE COMBATE SUPERIOR EN UN MOMENTO Y LUGAR DECISIVO	ACCIONES EN EL OBJETIVO
EXPLOTACIÓN DEL ÉXITO	INSTALACIÓN - COMANDO Y CONTROL
PROVEER SEGURIDAD E INTEGRIDAD A LAS FUERZAS	RECONOCIMIENTO

La **obtención y el mantenimiento de contacto con el enemigo**, busca ser permanente. Se lleva a cabo desde que se identifica el sistema objetivo, hasta que el ataque es detectado, y se espera haber cumplido con todos los pasos de la Cadena de Muerte, o no.

La **situación se aclara** cuando se finaliza el **reconocimiento**, y es el momento en el cual uno elige sus armas para atacar (**armamentización**). De lo contrario no se podrá llegar a atacar con grado de seguridad del daño que se vaya a ocasionar, por ende, no se podrá cumplir el objetivo.

La **explotación de la debilidad del enemigo** tiene su paralelo en la **explotación** de la vulnerabilidad del sistema, momento en el cual se hace el ingreso al mismo para continuar con la ejecución del ataque.

La **conquista y control de los RRCC** tiene su paralelismo con la **instalación**, proceso en el cual se lleva a cabo la instalación de aquellas herramientas, modificaciones de protocolos y parámetros, que permitirán llevar a cabo las acciones en el objetivo y lograr la persistencia sin ser detectados. Ya estamos sobre la altura.

La **retención de la iniciativa y la neutralización de la capacidad de reacción del adversario** se relacionan con un conjunto de procesos que, en el ámbito digital, suelen englobarse bajo el concepto de **Comando y Control (C2)**. Más que una fase aislada, C2 actúa como una capacidad transversal que comienza tras la instalación y se prolonga hasta las acciones finales sobre el objetivo. Su función es doble: por un lado, **mantener el impulso del ataque** a través de la persistencia y el movimiento lateral; por otro, limitar las posibilidades de respuesta del enemigo mediante la orquestación de acciones remotas que afectan directamente sus defensas. La robustez o fragilidad del C2 condiciona de manera decisiva la capacidad de sostener la iniciativa en el ciberespacio.

El **avance por el fuego y la maniobra** es similar al proceso de **explotación e instalación**, etapa en las cuales se explotan vulnerabilidades y se toma provecho de estas. También se podría trazar un paralelismo con el reconocimiento, aunque los objetivos que persiguen el reconocimiento, y el fuego y la maniobra, son distintos.

Otros principios encuentran un correlato más limitado. La **concentración de poder de combate superior**, relacionado con el principio de masa, difícil de reproducir en el plano digital, puede asociarse a la etapa de **acciones en el objetivo**, donde el atacante concentra sus efectos para maximizar el impacto. En cuanto a la **explotación del éxito**, esta se manifiesta tras haber penetrado en el sistema, utilizando la persistencia y los accesos obtenidos para multiplicar los efectos iniciales y ampliar el alcance de la operación (**instalación y comando y control**).

En resumen, si bien no todos los principios de la ofensiva tienen una equivalencia directa en la *Cyber Kill Chain*, el ejercicio de establecer este paralelismo permite demostrar la continuidad doctrinaria entre la guerra convencional y el ciberespacio. Un aspecto clave es la fase de Comando y Control, que se refiere a la capacidad técnica del atacante para establecer, mantener y utilizar canales de comunicación con el sistema comprometido. Esta función técnica es la que posibilita sostener la iniciativa, neutralizar defensas y explotar el éxito alcanzado, consolidando la ofensiva en el entorno cibernético.

4.3 Relación entre los conceptos de la Guerra de Maniobras y las Operaciones Ofensivas en el Ciberespacio.

En este punto vale recordar que las operaciones ofensivas en el ciberespacio se definen como acciones dirigidas a interferir, degradar, denegar o destruir sistemas de información enemigos (lo que afecta la confidencialidad, integridad y disponibilidad de la información). Su objetivo es producir efectos militares decisivos mediante medios digitales, a menudo sincronizados con otras dimensiones del conflicto (operaciones conjuntas o combinadas) para alcanzar los objetivos militares asignados.

Para este análisis se analizará como cumple, en particular una Operación Ofensiva en el Ciberespacio, con ciertos postulados doctrinarios de la Guerra de Maniobras, manifestados en la obra de William S. Lind, "*El manual de la Guerra de Maniobras*".

CONCEPTOS DE GUERRA DE MANIOBRAS	¿CUMPLE?
SUPERFICIES Y VACÍOS: Atacar la debilidad del enemigo con nuestro punto más fuerte	**Se busca explotar las vulnerabilidades del enemigo.**
ESFUERZO PRINCIPAL: Es el ataque principal, es único, unitario, y está dirigido hacia el objetivo.	**Se prepara una carga principal o payload.**
OBJETIVO: Fin hacia donde se dirige el accionar militar. Es el enemigo (Lidell Hart)	**El enemigo es un sistema de Información, persona o infraestructura.**
RESERVA: Elemento de combate decisivo para explotar un éxito.	**No cumple.**
TÁCTICA DE MISIONES: Decidir según la iniciativa a la luz del cumplimiento de la misión	**Puede, o no, cumplirlo.**

Puntualmente, destaco el concepto de reserva, dado que en mi apreciación no existe algo como tal en las operaciones en el ciberespacio. Las acciones se llevan a cabo de acuerdo a la oportunidad que se presenten, pero la planificación se hace para afectar a un sistema específico y con un propósito específico, para lo cual se prepara un payload, o "carga de combate" y es el esfuerzo principal.

Otro aspecto que quiero destacar es el de táctica de misiones, porque puede darse mucha libertad de acción, o pueden ser muy supervisada, sin libertad de acción, y esto estará determinado por la situación y el impacto esperado de la operación.

Si bien se analizó la aplicación de los conceptos de Guerra de Maniobras en las Operaciones Ofensivas en el Ciberespacio en particular, es importante destacar que como acciones contribuyentes a las operaciones en otros dominios las acciones en el ciberespacio potencian la guerra de maniobras, al permitir:

- Mayor velocidad en la toma de decisiones (OODA Loop): El ciclo OODA (Observar, Orientar, Decidir, Actuar) se acelera mediante inteligencia cibernética.
- Desorganización del enemigo sin contacto físico: Ciberataques pueden dejar al enemigo sin comunicaciones ni logística, facilitando avances rápidos.

- **Operaciones de engaño y confusión:** Manipulación de información y sistemas de mando puede inducir errores estratégicos en el oponente.
- **Coordinación en tiempo real:** Fuerzas distribuidas pueden sincronizar acciones con precisión a través de redes seguras.

4.4 Relación entre las fases de las Operaciones Ofensivas y las fases de una Operación Ofensiva en el Ciberespacio.

Finalmente, establecí un paralelismo entre las fases de las operaciones ofensivas, con las fases de un ciberataque de acuerdo con el marco visto. En base a ello, identifiqué los siguientes paralelismos.

<table>
<tr><th colspan="2">FASES DE UNA OPERACIÓN OFENSIVA</th><th>FASES DE UN CIBERATAQUE</th></tr>
<tr><td>Localización del enemigo</td><td rowspan="3">PREPARACIÓN</td><td rowspan="2">Reconocimiento (Activo - Pasivo)</td></tr>
<tr><td>Movimiento para establecer el contacto</td></tr>
<tr><td>Actividades tendientes a la preparación del ataque</td><td>Armamentización</td></tr>
<tr><td>Avance por acción del fuego y la maniobra.</td><td rowspan="5">ATAQUE</td><td>Entrega - Explotación</td></tr>
<tr><td>Asalto</td><td rowspan="3">Explotación - Instalación</td></tr>
<tr><td>Persecución por el fuego</td></tr>
<tr><td>Defensa inmediata</td></tr>
<tr><td>Reorganización</td><td>Comando y Control</td></tr>
<tr><td>Explotación</td><td>EXPLOTACIÓN</td><td rowspan="2">Acciones en el Objetivo</td></tr>
<tr><td>Persecución</td><td>PERSECUCIÓN</td></tr>
</table>

El cuadro establece un paralelismo conceptual entre las fases de una operación ofensiva convencional y las de un ciberataque, de acuerdo con el marco de la Cyber Kill Chain, evidenciando que, aunque se desarrollen en dominios distintos, ambas comparten una lógica estructural similar.

En la fase de **preparación**, la localización del enemigo y el movimiento para establecer contacto se corresponden con las actividades de **reconocimiento activo y pasivo** en el ciberespacio, destinadas a identificar vulnerabilidades, superficie de ataque expuesta al accionar del atacante y comprender la arquitectura del objetivo.

La **armamentización**, por su parte, entendida con la preparación de las "ciberarmas" para atacar a un enemigo, guarda cierto paralelismo con su contraparte de las operaciones ofensivas tradicionales, porque incluye actividades preparatorias para el accionar del ataque, como la concentración de fuego, movilidad o recursos logísticos.

En la fase de **ataque**, la maniobra combinada con fuego en una operación convencional encuentra su equivalente en la **entrega del vector de ataque y su explotación**, que marcan el momento de ruptura del sistema defensivo. Esta fase puede incluir desde un phishing o spear phishing, hasta vulnerabilidades tipo zero-day. Luego, se produce la **instalación del payload**, que permite establecer persistencia, acceso remoto o escalar privilegios. La fase culmina con el establecimiento de **comando y control (C2)**, lo que posibilita gobernar la operación desde fuera del entorno comprometido en forma persistente.

La fase de **explotación** en ambos contextos persigue la maximización de efectos: en el ámbito cinético, mediante la ruptura del frente, la dislocación táctica y la desorganización del adversario, mientras que en el ciberespacio, esta fase se traduce en las **acciones sobre el objetivo comprometido**: robo de información sensible, sabotaje, manipulación de datos, degradación de servicios, movimientos laterales dentro de la red o utilización del acceso para lanzar nuevos ataques.

La fase de **persecución**, como una fase de la ofensiva que se ejecuta contra una fuerza enemiga que se bate en retirada, una vez que ha perdido su capacidad de operar eficazmente, y tiene como finalidad destruirla por completo, impidiendo que se reconstituya o se retire ordenadamente, tiene su paralelismo con las acciones en el sistema objetivo del enemigo. Éstas pueden incluir acciones continuadas contra un sistema debilitado que intenta recuperar el control, contener la intrusión o aislar sus activos críticos. Esta persecución digital puede manifestarse como presión directa a través de sabotajes persistentes, corrupción de respaldos, propagación de malware o degradación sistemática. De esta forma se busca impedir que el defensor restablezca su capacidad operativa, consolidando así el éxito de la operación ofensiva y prolongando la pérdida de iniciativa del adversario.

5. Conclusiones.

Las operaciones ofensivas en el ciberespacio se han consolidado como un componente esencial de la guerra moderna. Su poder radica en que puede ser invisible, rápido, preciso y altamente disruptivo, afectando infraestructuras críticas, redes militares, sistemas económicos e incluso la percepción pública, sin necesidad de recurrir a la fuerza física directa.

Su ejecución eficaz no solo demanda personal altamente capacitado y conocimiento técnico especializado, sino también un marco doctrinal sólido que permita integrar estas acciones en el conjunto de las operaciones militares. Modelos como la *Cyber Kill Chain* cumplen un rol clave en este proceso, al ofrecer una estructura lógica y secuencial que facilita tanto la planificación ofensiva como la anticipación de acciones enemigas, promoviendo además la coordinación con los demás dominios operativos.

Lejos de ser un mero esquema técnico, la *Cyber Kill Chain* opera como un verdadero marco operativo-militar. Su valor reside en la capacidad para traducir dinámicas cibernéticas complejas a una lógica doctrinal comprensible, lo que permite identificar, anticipar y contrarrestar amenazas con mayor eficacia. En este sentido, las operaciones ofensivas en el ciberespacio comparten con las tradicionales el mismo propósito estratégico: quebrar la voluntad del adversario, neutralizar capacidades críticas o alcanzar objetivos político-estratégicos, aunque lo hagan desde un dominio distinto y con herramientas propias.

Los principios de la guerra —como la concentración del esfuerzo, la sorpresa, la economía de medios o la maniobra— mantienen plena vigencia en el ámbito cibernético, aunque adaptados a sus particularidades. Bajo una perspectiva de Guerra de Maniobras, los ciberataques buscan explotar vulnerabilidades específicas del enemigo, evitando sus defensas más robustas para generar efectos desproporcionados. Al igual que en las maniobras convencionales, el ataque cibernético debe contar con un esfuerzo principal claramente definido, generalmente representado por el *payload*, orientado a impactar un punto crítico del sistema adversario.

En este contexto, la táctica de misiones adquiere un protagonismo central: la descentralización operativa, la complejidad técnica del entorno y la necesidad de adaptabilidad exigen altos niveles de iniciativa, creatividad y autonomía por parte de quienes ejecutan estas operaciones. El objetivo último sigue siendo el mismo: degradar, neutralizar o destruir capacidades enemigas con el fin de imponer la propia voluntad.

No existe hoy una frontera nítida entre la guerra convencional y la guerra cibernética. Ambas se integran en un continuo operacional que exige a los planificadores y ejecutores una visión integral del conflicto. Por ello, resulta imprescindible formar cuadros militares capaces de comprender el ciberespacio como un campo de batalla más, con su propia geografía, fricción y niebla.

Comprender esta convergencia conceptual resulta clave para alcanzar la superioridad informacional y garantizar la libertad de acción en escenarios crecientemente interdependientes. Solo desde una comprensión profunda y doctrinalmente articulada del ciberespacio como dominio operativo, será posible diseñar y ejecutar operaciones ofensivas cibernéticas eficaces, bajo principios éticos y estratégicos claros.

Bibliografía

- Bermúdez, J. D. et al. (2022). *Técnicas Avanzadas de Ciberseguridad*.
- Zetter, K. (2014). *Countdown to Zero Day*. Crown Publishing.
- Buchanan, B. (2020). *The Hacker and the State*. Harvard University Press.
- Escuela de Guerra Naval. *Planeamiento Naval Operativo, Contribución Académica*.
- Arevalo Cuevas, E. J. *Cyber Kill Chain: Ataque y Defensa*.
- Mando Conjunto de Ciberdefensa – España. (2016). *¿Ciberespacio: nuevo campo de batalla?*
- TechLatest.net. *Reconnaissance – First Phase of Hacking*.
- Círculo Militar. *Manual de Guerra de Maniobras*.
- Robert Leonhard (2003), *The Principles of War for the Information Age*.

.

» Más noticias del mundo:

Agradecemos al CN Carlos Reynoso por su profusa compilación de noticias de temas de actualidad del quehacer naval. Pueden acceder a ella mediante el QR →

» 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.

Las opiniones vertidas en el presente son de exclusiva responsabilidad de sus autores, y no representan la opinión institucional de las entidades que se vinculan o aluden.