



**ACADEMIA DE GUERRA**

# ***Cuaderno de Difusión***

**Pensamiento de Estado Mayor**

**Horizontes estratégicos  
del campo de batalla  
actual: la seguridad,  
geopolítica, tecnología  
y logística**



Edición

**48**

Diciembre 2024 - ISSN 0717 - 4187



# **Cuaderno de Difusión del Pensamiento de Estado Mayor N° 48, año 2024.**

## **CONTENIDOS**

### **COMITÉ ACADÉMICO**

#### **Presidente:**

Coronel Manuel Provis Baker  
Director de la Academia de Guerra del  
Ejército de Chile.

#### **Secretario:**

Teniente Coronel Branko Versalovic Serrano,  
Jefe del CEEAG.

Dr. Mario Arteaga Velásquez, Centro de  
Graduados de la Academia de Guerra del  
Ejército de Chile (Chile)

Dra. Viana Figueroa Soto, Academia de  
Guerra del Ejército de Chile (Chile)

Dr. Marcos Jaramillo Contreras, Academia de  
Guerra del Ejército de Chile (Chile)

Dra. Carla Arce Ilabaca, Academia de Guerra  
del Ejército de Chile (Chile)

Dr. Jorge Sanz Jofré, Universidad del  
Desarrollo de Chile (Chile)

### **COMITÉ EDITORIAL**

Editor Responsable: Mg. Hernán Díaz  
Mardones, coordinador de asuntos  
académicos y administrativos del CEEAG.  
Mg. Alejandra Ilica Sepúlveda, investigadora y  
analista del CEEAG.

PC Javiera Pizarro Concha, encargada de  
plataforma publicaciones electrónicas.

Sof. Richard Pérez Espinosa, jefe de la Plana  
Mayor del CEEAG.

### **ARTÍCULOS:**

|                                                                                                                                                                            |    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| INGENIERÍA SOCIAL Y SUS IMPLICANCIAS EN LAS OPERACIONES<br>MILITARES: UN ANÁLISIS DESDE LA PERSPECTIVA DE LA<br>CIBERSEGURIDAD MILITAR<br>Mayor Carlos Bustamante Quintero | 7  |
| GUERRA AUTÓNOMA: EL COMIENZO DEL FIN<br>Mayor Claudio Herrera Sapunar                                                                                                      | 21 |
| IMPORTANCIA DEL APOYO LOGÍSTICO ANTICIPADO EN EL ÉXITO DE LAS<br>OPERACIONES DE PAZ<br>Mayor Esteban Vásquez Mulsow                                                        | 41 |
| MOVILIDAD ESTRATÉGICA: EL ROL DEL FERROCARRIL EN LA LOGÍSTICA<br>MILITAR<br>Mayor Sergio Villaseca Zanzi                                                                   | 59 |

“CUADERNO DE DIFUSIÓN, Pensamiento de Estado Mayor”, es editado y difundido por el Centro de Estudios Estratégicos de la Academia de Guerra del Ejército. Las ideas vertidas en los artículos contenidos en su interior son de exclusiva responsabilidad de los autores, y no representan necesariamente el pensamiento, doctrina o posición oficial del Ejército de Chile

## **Presentación del Director**

El Cuaderno de Difusión del Pensamiento de Estado Mayor, en su versión número 48, del año 2024, está conformado por 4 artículos enmarcados en el ámbito de las Ciencias Militares, para que, a través de su difusión, la Academia de Guerra, Instituto de Educación Superior del Ejército de Chile, coopere a incrementar el conocimiento en tópicos militares específicos e invite a la reflexión y al debate a sus alumnos y profesores principalmente, junto con la comunidad académica del sector de Seguridad y Defensa.

Los autores de los artículos que componen la presente publicación corresponden a Oficiales de Estado Mayor graduados de este Instituto, quienes luego de un riguroso proceso de investigación y posterior selección y validación por parte de la Academia de Guerra, presentan sus resultados finales.

De esta forma, el Mayor Carlos Bustamante Quintero, quien egresó como Oficial de Estado Mayor el año 2023, presenta el artículo titulado “Ingeniería social y sus implicancias en las operaciones militares: Un análisis desde la perspectiva de la ciberseguridad militar”, en el que se describe y analiza como la ingeniería social manipula el comportamiento humano, además, de las consecuencias de estos ataques pueden ser devastadoras comprometiendo la seguridad y la capacidad operativa de las fuerzas armadas.

A continuación, el Mayor Claudio Herrera Sapunar, quien egresó como Oficial de Estado Mayor el año 2023, colabora con el artículo titulado “Guerra Autónoma: El comienzo del fin”, el cual explora cómo la evolución de los Sistemas de Armas Autónomas Letales (LAWS) ha transformado la guerra moderna, comparando la ficción y sus respectivas secuelas con los avances tecnológicos actuales, situación que se puede apreciar claramente en los conflictos contemporáneos.

Posteriormente, el Mayor Esteban Vásquez Mulsow, quien egresó como Oficial de Estado Mayor en el año 2023, contribuye con el artículo “La importancia del apoyo logístico anticipado en el éxito de las operaciones de paz”, en este analiza la importancia del apoyo logístico anticipado para el éxito de las operaciones de paz, especialmente en contextos donde la infraestructura del país anfitrión ha sido gravemente dañada. Asimismo, considera que la planificación logística proactiva es fundamental para asegurar una respuesta efectiva ante las emergencias que afrontan las fuerzas desplegadas por ONU.

En el artículo final de este número, titulado “Movilidad estratégica: El rol del ferrocarril en la logística militar”, el Mayor Sergio Villaseca Zanzi, quien egresó como Oficial de Estado Mayor el año 2023, visualiza la importancia del ferrocarril para sostener las operaciones logísticas y la modernización de su infraestructura para asegurar una respuesta rápida en escenarios de crisis.

En síntesis, el presente Cuaderno de Difusión en su versión número 48 cumple con el objetivo de difundir el pensamiento de Estado Mayor, aplicado en diferentes tópicos del ámbito militar, ciberseguridad y la tecnología, constituyendo una fuente de consulta actualizada y vanguardista, que invita al debate y a la reflexión de los profesionales que estudian las Ciencias Militares.

Manuel Provis Baker  
Coronel  
Director de la Academia de Guerra



# INGENIERÍA SOCIAL Y SUS IMPLICANCIAS EN LAS OPERACIONES MILITARES: UN ANÁLISIS DESDE LA PERSPECTIVA DE LA CIBERSEGURIDAD MILITAR

*Social engineering and its implications in military operations: an analysis from the perspective of military cybersecurity*

Mayor Carlos Bustamante Quintero<sup>1</sup>

## Resumen

La ingeniería social (IS) constituye una amenaza latente para las operaciones militares, enfocándose en explotar las vulnerabilidades humanas para acceder a información sensible o interrumpir sistemas. A diferencia de los ataques técnicos, la IS manipula el comportamiento humano, haciendo difícil de contrarrestar. Las consecuencias de estos ataques pueden ser devastadoras, comprometiendo la seguridad y la capacidad operativa de las fuerzas armadas. Para mitigar los riesgos asociados a ataques mediante IS, se requiere un enfoque integral que combine capacitación continua del personal, implementación de tecnologías de seguridad avanzadas y la creación de políticas de seguridad dinámicas. Solo a través de la conciencia, la preparación y la adaptación constante, las fuerzas armadas podrán fortalecer su ciberseguridad y proteger sus sistemas críticos contra las amenazas de IS.

**Palabras clave:** Ingeniería social, operaciones militares, ciberseguridad, vulnerabilidades humanas.

## Abstract

Social engineering (SE) is a latent threat to military operations, focusing on exploiting human vulnerabilities to access sensitive information or disrupt systems. Unlike technical attacks, SE manipulates human behavior, making it difficult to counter. The consequences of these attacks can be devastating, compromising the security and operational capabilities of the armed forces. To mitigate the risks posed by being attacked through SE, a comprehensive approach is required that combines continuous training of personnel, implementation of advanced security technologies, and the creation of dynamic security policies. Only through awareness, preparedness, and constant adaptation will the armed forces be able to strengthen their cybersecurity and protect their critical systems against SE threats.

**Keywords:** Social engineering, military operations, cybersecurity, human vulnerabilities.

---

<sup>1</sup> Oficial de Estado Mayor del arma de Ingenieros, Especialista en inteligencia militar en el Ejército de Chile e inteligencia policial en Carabineros de Chile, Magister en Relaciones Internacionales, Seguridad y Defensa en la Academia Nacional de Estudios Políticos y Estratégicos y Licenciado en ciberseguridad en la Universidad Mayor. Correo electrónico: [carlos.bustamante.quintero@gmail.com](mailto:carlos.bustamante.quintero@gmail.com)

## Introducción

El advenimiento de la era digital ha modernizado el campo de batalla, trasladando las hostilidades al ciberespacio. En este nuevo escenario, las organizaciones militares se enfrentan a una amplia gama de amenazas cibernéticas que ponen en peligro la confidencialidad, integridad y disponibilidad de sus sistemas y datos. Entre estas amenazas, los ataques que emplean ingeniería social (IS), emergen como uno de los más sofisticados y difíciles de contrarrestar, explotando las vulnerabilidades psicológicas del ser humano para obtener información confidencial o acceso a sistemas restringidos, pudiendo comprometer a las instituciones de la defensa, afectando de esta forma a las operaciones militares.

La IS, puede definirse como *“el acto de manipular a una persona para que lleve a cabo una acción “que puede ser o no” lo más conveniente para el objetivo”* (Hadnagy C. , 2011, pág. 37), una definición más detallada indica que la IS puede entenderse como *“el conjunto de técnicas de tipo social que pueden usar ciertos individuos, grupos u organizaciones de cualquier tipo para manipular o persuadir a objetivos humanos, con la intención de que realicen acciones, tomen decisiones o revelen información valiosa para el atacante, en forma voluntaria”* (Ramos, Barbero, Marugan, & González, 2015, pág. 17).

Para los efectos de este artículo, y con la finalidad de mejorar el entendimiento a un nivel menos técnico, se definirá la IS como la manipulación psicológica de individuos para que revelen información confidencial o realicen acciones que comprometan la seguridad. Independiente a las definiciones, es indudable que la IS se ha convertido en un arma poderosa en el arsenal de los ciber atacantes. A diferencia de los ataques que explotan vulnerabilidades de hardware (físicas) o de software (lógicas), la ingeniería social se centra en el factor humano, aprovechando la confianza, la curiosidad y el miedo de las personas.

De acuerdo con lo anterior se plantea que el factor humano, debido a sus inherentes vulnerabilidades psicológicas, tales como la tendencia a apoyar o a servir, representa el eslabón más débil en la cadena de ciberseguridad militar. La IS, al explotar estas vulnerabilidades, y ser utilizadas como parte de un ataque mayor, constituye una amenaza significativa para las operaciones militares, poniendo en riesgo la confidencialidad de la información clasificada, la integridad de los sistemas de mando y control, y la disponibilidad de las infraestructuras críticas.

El presente artículo pretende reflexionar sobre la amenaza que la IS representa en las operaciones militares cuando es utilizada como parte de un ataque mayor y dar respuesta a la pregunta ¿Qué medidas pueden adoptar las organizaciones de la

defensa, especialmente chilenas, para fortalecer la ciberseguridad frente a las amenazas de la IS y proteger así la información clasificada, las operaciones militares y la reputación de las fuerzas armadas?

Para dar cumplimiento a lo anterior, en la primera parte se abordará la IS y sus tácticas, donde se analizarán las diferentes técnicas utilizadas por los ciberatacantes, como el *Phishing*, el *Tailgating* y el *Pretexting*, así como los objetivos y motivaciones de estos ataques, seguidamente se reflexionará sobre el factor humano como factor débil, donde se explorarán las vulnerabilidades psicológicas que hacen a las personas susceptibles a la manipulación social, y cómo estas pueden ser explotadas en el contexto militar. Posteriormente se abordará el impacto de la IS en las operaciones militares, donde se abarcarán las consecuencias de estos ataques en diferentes áreas de las operaciones militares, como la inteligencia, las comunicaciones y el mando y control y finalmente se presentarán algunas estrategias de mitigación, que propondrán medidas para fortalecer la ciberseguridad militar frente a las amenazas de la IS, incluyendo la concientización y capacitación del personal, el desarrollo de tecnologías de seguridad y la implementación de políticas y procedimientos de seguridad.

### **La ingeniería social y sus tácticas**

La ingeniería social, son técnicas que explotan las vulnerabilidades psicológicas del ser humano y se ha convertido en una de las principales amenazas para la ciberseguridad militar, cuando son utilizadas como parte de un ciberataque o un ataque físico. Los atacantes emplean una variedad de técnicas sofisticadas para manipular a las personas y obtener acceso a información confidencial o sistemas restringidos.

Tal como ya se ha señalado en la introducción del presente artículo, la IS utiliza al factor humano de una organización, para lograr sus objetivos, valiéndose de diferentes tácticas, a diferencia de los ataques cibernéticos tradicionales que se centran en vulnerabilidades técnicas, la IS explota la confianza, la curiosidad y el miedo de las personas.

Para lograr un mejor entendimiento, se describirán algunas de las tácticas de IS más utilizadas:

### *Phishing y Spear Phishing*

El *Phishing* consiste en el envío masivo de correos o mensajes, en los que se les solicita a los receptores, que ingresen a una página haciendo click en un link, todo lo anterior a través de una historia ficticia haciendo alusión a un premio, solicitud de información por parte de una entidad bancaria, posibilidad de corte de algún servicio por no pago, etc.

En el caso del *Spear Phishing*, se utiliza la misma táctica, sin embargo, esta no es masiva, se dirige a un objetivo específico, por lo que la historia ficticia que se utiliza para generar el ingreso al sitio web, es mucho más preparada y enfocada al objetivo.

En ambos casos, una vez dentro del sitio previamente generado, el cual cuenta con una estructura similar al original, se le puede solicitar al objetivo “...datos financieros, datos confidenciales, militares, o cualquier tipo de información que se encuentre dentro de una organización o empresa” (Ramos, Barbero, Marugan, & González, 2015, pág. 95). También se pueden solicitar datos personales que posteriormente son utilizados para generar otras credenciales como parte de un mayor ataque.

### *Tailgating*

El *Tailgating* es una táctica de IS bastante simple pero efectiva, que consiste en que un intruso no autorizado siga de cerca a una persona autorizada para acceder a un área restringida, aprovechando la apertura de puertas o torniquetes. Para esta técnica podría utilizarse algún tipo de indumentaria que hiciera “normal” su ingreso, de esta forma podría acceder a áreas donde se almacena información clasificada, equipos sensibles o sistemas de control, lo que podría permitirle obtener información valiosa, sabotear equipos o incluso llevar a cabo actos de espionaje. *Esta táctica se aprovecha de la “predisposición a sujetar la puerta al que viene detrás por motivos educacionales”* (Ramos, Barbero, Marugan, & González, 2015, pág. 29)

De igual forma una vez ingresando a un área que cuente con servidores, o computadores conectados a los sistemas de defensa, pueden conectarse dispositivos que, aprovechando alguna brecha de seguridad, puedan causar el robo de información o la vulneración de algún sistema para un ataque a mayor escala posterior.

## *Pretexting*

El *Pretexting* es una táctica de IS donde un atacante crea una historia falsa o un escenario convincente (pretexto) para manipular a una víctima y obtener información confidencial. *“Es más que simplemente producir una mentira; en algunos casos puede ser crear una identidad totalmente nueva y utilizarla para manipular al receptor de la información”* (Hadnagy C., 2023, pág. 91). Para el caso particular de las organizaciones militares, alguien podría hacerse pasar por un mando, un compañero de trabajo o incluso un proveedor para convencer a un funcionario de revelar datos confidenciales, como contraseñas, números de identificación o detalles sobre proyectos clasificados.

Las tácticas expuestas anteriormente solo son algunas de las muchas que pueden afectar las organizaciones, teniendo como denominador común, el aprovechamiento de las vulnerabilidades que presenta el ser humano para el logro de sus fines. Algo que hace aún más complicada su mitigación es que muchas de las cualidades que hacen vulnerable al ser humano, son aquellos valores y virtudes que son fomentadas en la vida en sociedad, tales como la confianza, el respeto hacia los adultos, la bondad, etc. Derivado de lo anterior la concientización y formación, son imprescindibles para mitigar los riesgos que atacan al factor humano de una organización.

## **El factor humano como eslabón débil**

“El Ingeniero social, o atacante diestro en el arte del engaño, se alimenta de las mejores cualidades de la naturaleza humana: nuestra tendencia a servir de ayuda y apoyo, a ser educado, a colaborar y el deseo de concluir un trabajo” (Mitnick & Simon, 2006, pág. 299)

Una de las razones por las cuales la IS es tan efectiva, es la naturaleza misma del ser humano. Nuestras predisposiciones psicológicas, como la confianza, la reciprocidad y la urgencia, pueden ser explotadas por los atacantes para lograr sus objetivos. Tal como se mencionaba anteriormente, las vulnerabilidades que presenta el ser humano frente a los ataques que emplean IS no deben confundirse con deficiencias, sólo cuando se carece de una formación orientada a la seguridad, políticas adecuadas, además de un apoyo tecnológico suficiente, los valores y virtudes que posee el ser humano y que son aquellos que nos permiten vivir en sociedad, se transforman en vulnerabilidades, que aprovechadas por la IS, se transforman en amenazas a las organizaciones, en este caso particular, de defensa.

La confianza constituye un pilar fundamental en las interacciones humanas, pero en el ámbito de la ciberseguridad se erige como una vulnerabilidad explotable. Los atacantes suelen aprovechar la credibilidad que las personas depositan en entidades reconocidas para perpetrar engaños. Como acertadamente señala Kevin Mitnick, *"establecer la credibilidad es el primer paso en la mayoría de los ataques de ingeniería social"* (2006, pág. 314). Al cultivar una apariencia de cercanía y confianza, los atacantes logran manipular a sus objetivos para que revelen información sensible o concedan accesos que, a priori, parecen inofensivos. Sin embargo, estos datos suelen ser piezas clave en un rompecabezas más amplio, permitiendo a los atacantes escalar sus operaciones o validar hipótesis cruciales para sus organizaciones.

La confianza y el principio de reciprocidad constituyen dos pilares fundamentales de las relaciones humanas que, paradójicamente, se erigen como vulnerabilidades significativas en el ámbito de la ciberseguridad. Los atacantes, conscientes de esta dinámica, explotan hábilmente estas tendencias para manipular a sus víctimas y lograr sus objetivos maliciosos. Como señala Hadnagy (2023, pág. 131), al ofrecer un beneficio previo, como información gratuita o un favor, los ciberdelincuentes incrementan considerablemente la probabilidad de que sus solicitudes sean atendidas. Este mecanismo psicológico, conocido como reciprocidad, funciona como un ciclo vicioso: al conceder algo, el atacante genera en la víctima una sensación de deuda, lo que facilita que esta acceda a posteriores peticiones, impulsada por el deseo de equilibrar la balanza. Para explotar eficazmente esta vulnerabilidad, los atacantes suelen identificar o generar una necesidad específica en sus objetivos, estableciendo al mismo tiempo un lazo de confianza que les permita posicionarse como la solución a dicho problema. De esta manera, los cibercriminales pueden llevar a cabo sus ataques de manera más sutil y efectiva, aprovechando la predisposición humana a devolver favores.

Por otro lado, la urgencia y el miedo son emociones poderosas que pueden nublar el juicio de las personas. *"Nuestro cerebro está condicionado para reaccionar rápidamente ante una amenaza, el miedo es una de nuestras emociones básicas y, sin duda, nos lleva a tomar muchas decisiones"* (Deutsch, 2022, pág. 20). Los atacantes a menudo crean un sentido de urgencia o miedo para presionar a las víctimas a tomar decisiones apresuradas y sin pensar en las consecuencias. Por ejemplo, un mensaje que advierte sobre una cuenta bancaria bloqueada puede llevar a una víctima a revelar su contraseña sin verificar la autenticidad del mensaje.

Además de la confianza, la reciprocidad y el miedo, existen otras vulnerabilidades psicológicas que pueden ser explotadas por los atacantes, como:

- La autoridad, donde las personas tienden a obedecer a figuras de autoridad, incluso cuando las órdenes son claramente erróneas, es un principio psicológico que los atacantes aprovechan. De igual manera, la escasez, que genera una urgencia debido a que los recursos son limitados o alguna oferta tiene una duración determinada, puede llevar a las personas a tomar decisiones impulsivas y poco racionales.
- Por otro lado, la simpatía, ese sentimiento que nos inclina a ayudar a aquellos que percibimos como similares a nosotros o que se encuentran en una situación difícil, también es una herramienta poderosa en manos de los ciberdelincuentes. Al generar empatía, los atacantes pueden manipular a sus víctimas para que revelen información confidencial o realicen acciones que beneficien al atacante. Estos principios psicológicos, cuando son explotados de manera estratégica, pueden convertirse en poderosas armas en el arsenal de los cibercriminales, facilitando la ejecución de ataques de ingeniería social altamente efectivos.

Los sentimientos, principios y características humanas antes mencionados, normalmente son identificados como valores o virtudes, y no nos equivoquemos, lo son, sin embargo, cuando se carece del conocimiento, las políticas y la tecnología, pueden transformarse en el punto de entrada de un atacante. Las instituciones armadas o relacionadas a la defensa, no se encuentran ajenas a estos ataques que, de ser exitosos, pueden afectar gravemente a las operaciones militares.

### **Impacto de la ingeniería social en las operaciones militares**

Los objetivos de los ataques de IS en el ámbito militar son diversos y pueden incluir el robo de información clasificada, el sabotaje de sistemas, el espionaje, la desinformación y la propaganda. Estos ataques pueden tener consecuencias devastadoras para las operaciones militares y la seguridad nacional.

La IS, lejos de ser una amenaza exclusiva del ámbito civil, ha penetrado profundamente en el dominio militar, con consecuencias potencialmente catastróficas para las operaciones. Los atacantes, ya sean actores estatales, no estatales o cibercriminales, emplean tácticas de IS para infiltrarse en redes militares, robar información clasificada, sabotear sistemas críticos y, en última instancia, socavar la capacidad de respuesta y la toma de decisiones de las fuerzas armadas.

Uno de los impactos más directos de la ingeniería social en el ámbito militar es la pérdida de información clasificada. A través de técnicas como el *phishing* y el *spear phishing*, los atacantes pueden engañar a miembros del personal militar para que

revelen contraseñas, credenciales de acceso o información sensible sobre operaciones en curso. Esta filtración de información puede comprometer misiones, poner en peligro vidas y dañar la reputación de una nación (Ross & Pillitteri, 2024).

Un ejemplo paradigmático de cómo la IS se ha utilizado como arma en conflictos contemporáneos lo encontramos en los ciberataques sufridos por Georgia durante el conflicto con Rusia en las regiones separatistas de Osetia del Sur y Abkhazia. Si bien los ataques a los sitios web del gobierno georgiano, que resultaron en su indisponibilidad o en la manipulación de su contenido para propagar desinformación, pueden parecer meramente técnicos, es fundamental comprender que detrás de ellos se esconden sofisticadas estrategias de IS. Al privar a la población de información veraz y confiable, los atacantes buscaron sembrar la confusión, erosionar la confianza en las instituciones gubernamentales y manipular la opinión pública, lo que a su vez debilitó la capacidad de respuesta del gobierno georgiano ante la crisis. Estos ataques no solo tuvieron un impacto directo en la infraestructura digital del país, sino que también representaron una forma de guerra psicológica, donde la información se convirtió en un arma de doble filo (Díaz del Río, 2011)

Los sistemas de mando, control, comunicaciones, computación e inteligencia (C4I)<sup>2</sup> son fundamentales para las operaciones militares modernas. Al infiltrarse en estos sistemas, los atacantes pueden causar interrupciones significativas, como la interrupción de las comunicaciones, la pérdida de datos críticos o el control remoto de sistemas de armas. (Marowski, 2018, pág. 122)

Un ejemplo notable es el ataque Stuxnet, que utilizó un malware altamente sofisticado para sabotear las centrifugadoras de enriquecimiento de uranio en Irán, en este ataque se utilizó un pendrive<sup>3</sup>, la cual contenía un malware<sup>4</sup>, este al ser instalado en el sistema produjo una lectura errónea de las revoluciones de las turbinas que enfriaban el agua del reactor, lo que generó un sobrecalentamiento y su inutilización. (Silva, 2018, pág. 304)

---

<sup>2</sup> Por sus siglas en Inglés *Command, Control, Communications, Computers e Intelligence*, El término **C4I** abarca las tecnologías y estrategias que ayudan a coordinar, comunicar, y controlar las fuerzas militares, integrando datos de inteligencia para apoyar la toma de decisiones en tiempo real. Es un componente clave en las operaciones militares modernas, permitiendo una comunicación y análisis efectivo en el campo de batalla y mejorando la eficiencia y efectividad de las misiones (Marowski, 2018)

<sup>3</sup> Memoria Extraíble

<sup>4</sup> Software de índole malicioso, como un virus, gusano, caballo de troya, etc.

Lo más interesante de este caso es la sofisticada combinación de ingeniería social y ciberataque. Para llevar a cabo la infección inicial, los atacantes explotaron una vulnerabilidad humana fundamental, la curiosidad. Mediante la IS, lograron obtener información crucial sobre el software utilizado en el sistema de control de las turbinas. Posteriormente, un dispositivo de almacenamiento infectado (un pendrive) fue estratégicamente dejado en un lugar accesible para los operadores de la planta, con la esperanza de que alguien lo conectara a un equipo de control. Al hacerlo, el malware contenido en el dispositivo se propagó por el sistema, manipulando las lecturas de las turbinas y provocando su sobrecalentamiento. Este ejemplo ilustra cómo la IS puede servir como la puerta de entrada para ciberataques altamente destructivos, donde la explotación de la confianza y la curiosidad humanas se convierte en un elemento fundamental del ataque.

La IS también se utiliza para difundir desinformación y propaganda entre las fuerzas armadas y la población civil. Los atacantes pueden crear cuentas falsas en redes sociales, difundir noticias falsas o manipular la opinión pública para sembrar la discordia y socavar la moral. Este tipo de ataques pueden tener un impacto psicológico significativo en las tropas y afectar su cohesión, logrando el objetivo que es afectar al factor humano en las operaciones, disminuyendo el apoyo a las operaciones por parte de la población y con esto afectando la voluntad política. Uno de estos casos se vivió en la operación Tormenta del Desierto, donde el Ejército Estadounidense logra interceptar las comunicaciones de los comandantes del Ejército Iraquí, enviando mensajes que los desconcertaban y evidenciaban la mala seguridad de sus sistemas, haciendo decaer la moral en las tropas que podían escuchar como los soldados norteamericanos hablaban en sus frecuencias y detectaban sus movimientos (Mitnick & Simon, 2006, pág. 338).

### **Estrategias de mitigación**

La IS cuando es utilizada como parte de un ciberataque o ataque físico, representa una amenaza constante y evolutiva para las organizaciones militares. Para hacer frente a esta amenaza, es necesario implementar una serie de medidas de seguridad que abarquen tanto el aspecto humano como el tecnológico. A continuación, se detallan tres estrategias de mitigación clave: capacitación y formación, uso de tecnologías y elaboración de políticas.

Como señala el NIST (National Institute of Standards and Technology)<sup>5</sup> en su publicación 800-171, la capacitación debe ser continua y adaptada a las nuevas amenazas emergentes (NIST, 2021), es por esto por lo que la **capacitación y formación del personal**, son elementos fundamentales para fortalecer la resistencia ante los ataques de ingeniería social. Un programa de capacitación efectivo debe incluir la concientización sobre las tácticas de ingeniería social, derivado de esto, es necesario que todo el personal que se emplea en los organismos de la defensa sea consciente de las técnicas más comunes utilizadas por los atacantes, esto implica la realización de academias (charlas, exposiciones, etc.) que permitan conocer las tácticas y técnicas más utilizadas por los atacantes que emplean la IS para llevar a cabo sus objetivos.

Otra forma de implementar medidas que cooperen en la mitigación de ataques de IS son las simulaciones y ejercicios prácticos, estos permiten al personal poner en práctica los conocimientos adquiridos y desarrollar habilidades para identificar y responder a situaciones de riesgo, lo anterior sumado a pruebas de penetración, ayudan a identificar las vulnerabilidades humanas y técnicas de una organización, permitiendo así tomar medidas correctivas.

Si bien es imposible eliminar por completo las vulnerabilidades humanas, existen medidas que pueden ayudar a reducir el riesgo de ser víctimas de ataques de ingeniería social, este es el caso de la verificación de la información, la cual consiste en verificar la autenticidad de la fuente antes de hacer clic en un enlace, descargar un archivo o proporcionar información confidencial. Otra forma de mitigación de las vulnerabilidades humanas es la desconfianza saludable, donde lo importante es ser escépticos ante cualquier solicitud que parezca sospechosa. Todas estas medidas solo pueden implementarse con una adecuada capacitación y formación del personal que maneja o tiene acceso a información que pueda ser explotada por un atacante mediante el empleo de IS.

Para garantizar la seguridad de una organización es fundamental comprender cómo la seguridad tecnológica interactúa con otras estrategias de seguridad (Avigilon, 2024). En este sentido, las tecnologías de la información desempeñan un papel crucial en la mitigación de los riesgos asociados con la ingeniería social. Una de las medidas más comunes es el empleo de filtros de correo electrónico, capaces de identificar y bloquear correos electrónicos sospechosos antes de que lleguen a las bandejas de entrada de los usuarios. Asimismo, los sistemas de detección de

---

<sup>5</sup> El Instituto Nacional de Estándares y Tecnología (NIST) fue fundado en 1901 y ahora forma parte del Departamento de Comercio de Estados Unidos. NIST es uno de los laboratorios de ciencias físicas más antiguos del país.

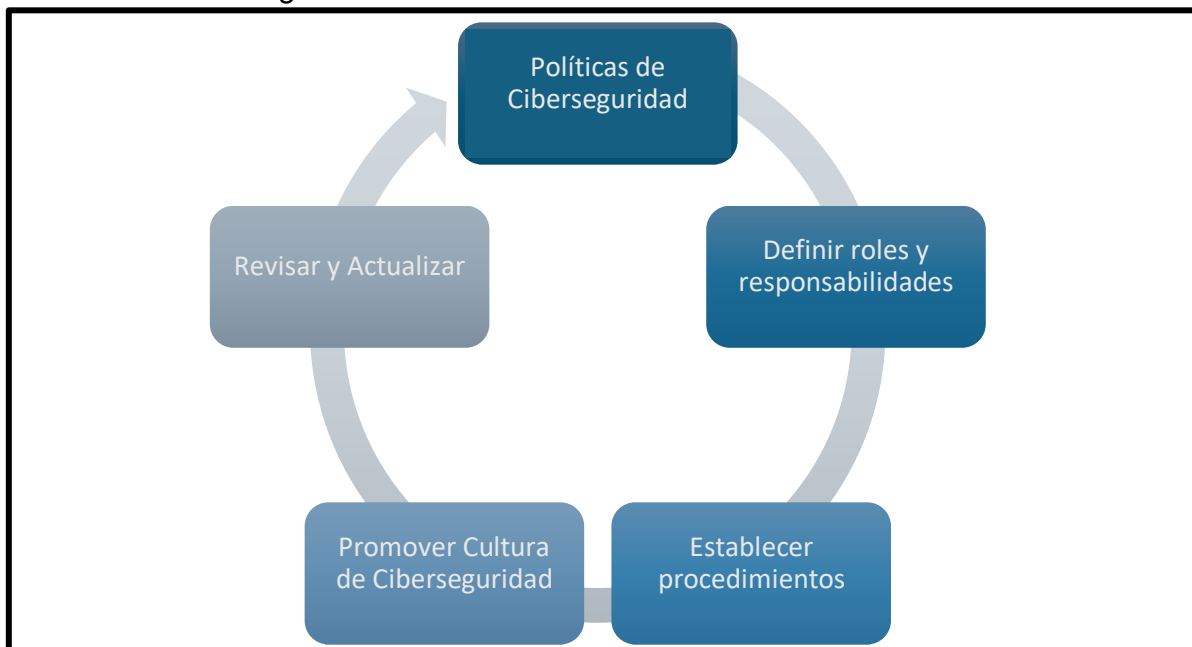
intrusiones juegan un papel fundamental al monitorear continuamente las redes en busca de actividades anómalas. Finalmente, la autenticación multifactorial añade una capa adicional de seguridad, exigiendo a los usuarios que presenten múltiples credenciales para acceder a los sistemas. Al combinar estas tecnologías, las organizaciones pueden crear una defensa en profundidad que dificulta significativamente el éxito de los ataques de ingeniería social.

No obstante, como acertadamente señala Kevin Mitnick y Simon (2006), “una compañía puede gastar cientos de miles de euros en firewalls, sistemas de cifrado y demás tecnologías de seguridad, pero si un atacante engaña a un empleado, todo ese dinero no habrá servido para nada”. Esta afirmación, aunque pueda parecer contradictoria a la luz de lo expuesto anteriormente, resalta un hecho innegable, el ser humano sigue siendo el eslabón más débil en cualquier cadena de seguridad. Por ello, resulta fundamental complementar las medidas tecnológicas con una sólida estrategia de concientización y formación de los empleados. La elaboración, implementación y seguimiento de políticas de seguridad sólidas constituye el pilar fundamental de cualquier programa de ciberseguridad, ya que proporciona un marco de referencia claro y conciso para guiar las acciones de todos los miembros de la organización.

A juicio de este autor, para que una política de seguridad sea efectiva, debe contar con al menos cuatro factores interrelacionados que la conviertan en un ciclo virtuoso. En primer lugar, es necesario definir claramente los roles y responsabilidades de cada miembro del personal en materia de seguridad. Posteriormente, se deben establecer procedimientos detallados para la gestión de incidentes, la respuesta a emergencias y la recuperación ante desastres. Estos procedimientos deben ser claros, concisos y fácilmente accesibles. En tercer lugar, es fundamental promover una cultura de seguridad en toda la organización. Esta cultura debe arraigarse en todos los niveles, desde la alta dirección hasta los empleados de primera línea. Finalmente, las políticas de seguridad deben ser revisadas y actualizadas periódicamente para adaptarse a los cambios constantes en el entorno de amenazas cibernéticas.

**FIGURA N° 1**

*Ciclo Política de Seguridad*



*Nota: Elaboración propia.*

## **Conclusión**

El análisis de la ingeniería social (IS) y sus implicancias en las operaciones militares desde la perspectiva de la ciberseguridad, revela una amenaza multifacética y persistente que se centra en el eslabón más débil de la seguridad, el factor humano. La IS explota las vulnerabilidades psicológicas inherentes al ser humano, como la confianza, la reciprocidad y el miedo, utilizando técnicas sofisticadas como el *phishing*, el *tailgating* y el *pretexting* para obtener acceso a información confidencial o sistemas restringidos. A diferencia de los ataques que explotan vulnerabilidades técnicas, la IS se focaliza en manipular el comportamiento humano, lo que la convierte en una de las amenazas más difíciles de contrarrestar dentro del ciberespacio militar.

Uno de los aspectos más preocupantes es que los ataques de que emplean IS no solo buscan la obtención de información, sino que también pueden tener un impacto devastador en las operaciones militares. La pérdida de información clasificada, la disrupción de sistemas de mando y control, y la propagación de desinformación y propaganda son algunos de los efectos que pueden comprometer gravemente la capacidad operativa y la seguridad de una nación. Ejemplos como el ataque Stuxnet o los ciberataques en el conflicto entre Georgia y Rusia demuestran cómo la IS

puede ser empleada para sabotear infraestructuras críticas y desestabilizar a las fuerzas armadas a través de la manipulación del factor humano.

Ante esta realidad, la mitigación de los riesgos asociados a la IS en el contexto militar requiere un enfoque integral que abarque tanto la capacitación y concientización del personal como el desarrollo e implementación de tecnologías de seguridad robustas y la elaboración de políticas de seguridad rigurosas. La capacitación continua del personal es crucial para que los individuos sean conscientes de las tácticas utilizadas por los atacantes y puedan reconocer y resistir intentos de manipulación. Las simulaciones y ejercicios prácticos también juegan un papel esencial en el fortalecimiento de la resiliencia ante ataques de IS, permitiendo al personal experimentar escenarios de riesgo en un entorno controlado y desarrollar habilidades de respuesta efectiva.

Desde un punto de vista tecnológico, el uso de herramientas como filtros de correo electrónico avanzados, sistemas de detección de intrusiones y autenticación multifactorial son medidas esenciales para reducir la exposición a ataques de IS. Estas tecnologías actúan como barreras adicionales que dificultan la ejecución de tácticas de IS y protegen la información sensible al exigir múltiples capas de verificación y monitoreo constante de actividades sospechosas.

Finalmente, las políticas de seguridad deben ser claras, exhaustivas y dinámicas, adaptándose continuamente a las nuevas amenazas emergentes. Estas políticas no solo deben establecer protocolos de acción en caso de un ataque, sino también fomentar una cultura de seguridad en toda la organización, donde la ciberseguridad sea vista como una responsabilidad compartida por todos los miembros de las fuerzas armadas.

En conclusión, los ataques que emplean la ingeniería social representan una amenaza significativa para las operaciones militares, pero con un enfoque multidimensional que combine la capacitación, la tecnología y las políticas adecuadas, es posible fortalecer la ciberseguridad y proteger la integridad y disponibilidad de los sistemas y datos militares. La naturaleza evolutiva de las amenazas cibernéticas exige una constante adaptación y mejora de las estrategias de defensa, asegurando que las fuerzas armadas estén preparadas para enfrentar los desafíos del ciberespacio en un entorno cada vez más complejo y hostil.

## Referencias

- Avigilon. (2024). *Guía Tecnológica de Seguridad: Tendencias del sector para el 2024*. Obtenido de Tendencias en tecnologías de seguridad: <https://www.avigilon.com/es/blog/security-technology>
- Deutsch, V. (2022). *Ciberseguridad Para Directivos*. España: Almuzara.
- Díaz del Río, J. J. (2011). *La Ciberseguridad en el Ámbito Militar*. Cuadernos de Estrategia N°149, 215-256.
- Díaz, H. (2018). *Infraestructura Crítica Vulnerable a la Ciberguerra*. La Ciberguerra, Sus Impactos y Desafíos, 45-58.
- Equipo CEEAG. (2018). *Desafíos Para Afrontar la Ciberguerra*. La Ciberguerra, Sus Impactos y Desafíos, 147-164.
- Hadnagy, C. (2011). *Ingeniería Social: El Arte Del Hacking Personal*. Madrid: ANAYA.
- Hadnagy, C. (2023). *Ingeniería Social, La Ciencia de la Piratería Humana*. Madrid: ANAYA.
- Marowski, C. (2018). *Efectos de los Riesgos y Amenazas de la Ciberguerra en la Infraestructura Crítica*. La Ciberguerra, Sus Impactos y Desafíos, 107-128.
- Mauricio, F. (2023). *Cyberceo, Una Visión Estratégica de la Ciberseguridad*. España: Marcombo.
- Mitnick, K., & Simon, W. (2006). *El Arte de la Intrusión, La Verdadera Historia de las Hazañas de Hackers, Intrusos e Impostores*. Madrid: RA-MA.
- Mitnick, K., & Simon, W. (2013). *Un Fantasma en el Sistema*. Madrid: Capitán Swing Libros.
- Mitnick, K., & Vamosi, R. (2023). *El Arte de la Invisibilidad*. Madrid: ANAYA.
- Ramos, A., Barbero, C., Marugan, D., & González, I. (2015). *Conoce Todo Sobre Hacking con Ingeniería Social: Técnicas para Hackear Humanos*. Madrid: RA-MA.
- Ross, R., & Pillitteri, V. (2024). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. USA: NIST.
- Silva, F. (2018). Stuxnet - *El Software como Herramienta de Control Geopolítico*. Revista PUCE (106), 297-314.

# GUERRA AUTÓNOMA: EL COMIENZO DEL FIN

*Autonomous war: the beginning of the end*

Mayor Claudio Herrera Sapunar<sup>1</sup>

**Resumen:** El artículo explora cómo la evolución de los Sistemas de Armas Autónomas Letales (LAWS) ha transformado la guerra moderna, comparando la ficción distópica de Terminator (1984) y sus respectivas secuelas con los avances tecnológicos actuales. A través de ejemplos recientes en los conflictos de Rusia-Ucrania e Israel-Hamás, se analiza el impacto del empleo de drones autónomos y softwares en el campo de batalla. Estos desarrollos plantean serias ventajas militares, pero también, dejan en evidencia inquietudes éticas y legales sobre la deshumanización de la guerra y la autonomía de las máquinas para tomar decisiones letales. El artículo concluye que la comunidad internacional debe actuar para regular estas tecnologías y preservar los principios éticos fundamentales en los conflictos armados.

**Palabras clave** Guerra autónoma - Sistemas Autónomos de Armas Letales - Guerra futura.

**Abstract:** The article explores how the evolution of Lethal Autonomous Weapon Systems (LAWS) has transformed modern warfare, comparing the dystopian fiction of Terminator (1984) and its respective sequels with current technological advances. Through recent examples in the Russia-Ukraine and Israel-Hamas conflicts, the impact of autonomous drones and software on the battlefield is analyzed. These developments present serious military advantages but also highlight ethical and legal concerns regarding the dehumanization of war and the autonomy of machines to make lethal decisions. The article concludes that the international community must act to regulate these technologies and preserve fundamental ethical principles in armed conflicts.

**Keywords:** Autonomous Warfare - Lethal Autonomous Weapons Systems - Future warfare.

---

<sup>1</sup> Oficial de Estado Mayor del arma de Infantería, Especialista en Paracaidismo Básico, Comandos, Inteligencia y Guerra Especial mención Liderazgo. Profesor de Academia en Historia Militar y Estrategia. Se ha desempeñado en diversas áreas de las Operaciones Especiales y fue comandante de la Agrupación de Fuerzas Especiales. Correo electrónico: [claudio.herreras@ejercito.cl](mailto:claudio.herreras@ejercito.cl)

## Introducción

Cuando la película *Terminator* se estrenó en 1984, la humanidad fue confrontada por primera vez con una visión apocalíptica de lo que los sistemas autónomos, impulsados por inteligencia artificial, podrían significar para el futuro de nuestra especie. La idea de la existencia de máquinas capaces de tomar decisiones letales por sí mismas, sin intervención humana, capturó la imaginación de millones, sembrando la inquietud sobre un futuro donde la tecnología podría volverse incontrolable. A más de tres décadas del estreno de *Terminator* y sus respectivas secuelas, la realidad se ha acercado peligrosamente a esa ficción, con el desarrollo e implementación de sistemas autónomos de armas letales (LAWS, por su sigla en inglés) en conflictos modernos.

El progreso de la inteligencia artificial (IA) ha permitido la creación de armas que no solo cumplen órdenes, sino que pueden identificar y atacar objetivos por cuenta propia. En la guerra entre Rusia y Ucrania, se ha evidenciado el uso de enjambres de drones navales autónomos en ataques contra la flota rusa en el Mar Negro, demostrando la capacidad de coordinar múltiples unidades sin intervención humana directa. En el conflicto entre Israel y Hamás, sistemas como el software *Lavender*, que permite la identificación automática de amenazas en tiempo real, y el drone *Lanius*, diseñado para explorar entornos complejos y seleccionar objetivos para ataques precisos, han marcado un punto de inflexión en la guerra moderna. Ambos ejemplos, ilustran el alcance y la sofisticación que han alcanzado los LAWS, y plantean inquietantes preguntas sobre la creciente deshumanización de la guerra y los riesgos éticos y estratégicos asociadas a esta tecnología. Entre ellas ¿Estamos avanzando hacia un futuro donde la guerra será de manera autónoma, librada por máquinas que toman decisiones letales de manera independiente?

En este artículo, exploraremos el concepto de *guerra autónoma*, definida como la utilización de sistemas autónomos en el campo de batalla, capaces de operar sin supervisión humana directa y tomar decisiones en tiempo real. Estos LAWS abarcan todos los dominios físicos e incluyen tecnologías avanzadas para la adquisición de objetivos como el software *Lavender*. Analizaremos cómo estos sistemas pueden identificar y atacar objetivos sin intervención humana.

Otro aspecto relevante será la revisión de los argumentos a favor y en contra de su implementación. Los defensores de los LAWS argumentan que estas tecnologías pueden reducir la cantidad de víctimas humanas en los conflictos, minimizar los errores en el combate y permitir una respuesta más rápida y precisa. Además, sugieren que la automatización puede limitar el riesgo para los soldados en el campo de batalla. Por su parte, los críticos advierten sobre los peligros éticos que

representa el hecho de delegar decisiones de vida o muerte a máquinas, la ausencia de rendición de cuentas en caso de fallos y la posibilidad de iniciar una carrera armamentista descontrolada que pueda desestabilizar la seguridad global.

A lo largo de este artículo, se examinarán estos temas en profundidad, proporcionando una visión crítica de la evolución de los LAWS y las implicaciones de la *guerra autónoma* en el mundo contemporáneo.

## **Una nueva era de la guerra**

Estamos a punto de entrar en una era completamente nueva de la guerra, una en la que los sistemas autónomos y no tripulados dominarán el campo de batalla. Estos sistemas reemplazarán a los actuales vehículos aéreos, navales y terrestres en todos los dominios operacionales y el espectro de las operaciones militares. Un régimen como este podría alterar fundamentalmente la forma en que se concibe la estrategia de defensa e influir en cómo los responsables de la toma de decisiones evalúan las ventajas y desventajas del uso de la fuerza. Actualmente, se encuentran en desarrollo muchas discusiones sobre los principios operacionales y tácticos, la conexión entre las acciones ofensivas y defensivas, y las ramificaciones morales y éticas de la implementación de tales sistemas, previendo que estas seguramente seguirán por un buen tiempo y sin una definición clara por parte de los involucrados.

El empleo de vehículos ya sea terrestres, aéreos o marítimos no tripulados armados sigue siendo un tema controvertido en las discusiones sobre el futuro de la guerra. Solo unas pocas naciones han desplegado tales sistemas y muchos gobiernos se oponen al uso de estas tecnologías por motivos morales. No solo los sistemas futuros serán autónomos, sino que no habrá humanos involucrados en el proceso de toma de decisiones en absoluto. Este hecho es lo que actualmente causa la mayor preocupación en la comunidad internacional y sin duda genera opiniones divididas.

La ética y el marco legal que rigen los conflictos armados se basa en el concepto de *guerra justa*, el que también puede dar cabida al empleo de los sistemas autónomos que están actualmente en desarrollo. Según las leyes de la *guerra*, el uso apropiado de la fuerza se determina considerando tanto la proporcionalidad de la fuerza empleada como su resultado (Naciones Unidas, 2023). Resultaría éticamente problemático que un sistema autónomo causara la muerte de un civil. Sin embargo, su muerte habría sido moral y legalmente justificada si la fuerza aplicada hubiera sido considerada apropiada dadas las circunstancias y la amenaza. En ese sentido, cuando los sistemas autónomos están diseñados para

seguir las reglas de la guerra, es muy probable que no se creen nuevos dilemas morales al ser utilizados en combate.

### **Algunas definiciones de guerra autónoma**

Según el Centro de Estudios Estratégicos e Internacionales (CSIS en inglés), la *guerra autónoma* se define como un tipo de conflicto armado en el que se utilizan sistemas de armas y tecnologías que pueden operar y tomar decisiones sin la intervención humana directa. Estos sistemas pueden identificar, seleccionar y atacar objetivos de manera independiente, basándose en algoritmos de inteligencia artificial, sensores y aprendizaje automático. La *guerra autónoma* difiere de los conflictos tradicionales en que la toma de decisiones sobre el uso de la fuerza se delega en máquinas, lo que plantea importantes dilemas éticos y operacionales (Center for Strategic and International Studies, 2022).

De la misma forma, el Comité Internacional de la Cruz Roja (CICR), desde una perspectiva más ética y moral, define el término *guerra autónoma* como la participación de sistemas autónomos de armas en combate, donde las decisiones críticas sobre objetivos militares se delegan a máquinas sin supervisión humana. Desde un punto de vista humanitario y legal, esto plantea preocupaciones sobre la capacidad de tales sistemas para cumplir con el derecho internacional humanitario, especialmente en lo que respecta a la distinción entre combatientes y civiles y la proporcionalidad de los ataques (Comité Internacional de la Cruz Roja, 2022).

Por otra parte, y con un enfoque más militar, la Universidad de Queensland, entiende que la *guerra autónoma* implica el uso de tecnologías autónomas en conflictos, donde los sistemas no solo realizan tareas operativas, sino que toman decisiones tácticas y estratégicas sin intervención humana. Estos sistemas pueden incluir drones, municiones merodeadoras y otros vehículos autónomos que se encargan de misiones de reconocimiento, ataques y defensa. En este contexto, la *guerra autónoma* supone una disrupción radical de la forma en que se libran los conflictos, dado que las decisiones de combate ya no dependen exclusivamente del juicio humano (The University of Queensland, 2021).

Consecuente con las definiciones anteriores, para este artículo se entenderá por *guerra autónoma* lo siguiente:

*Un tipo de conflicto armado en el que se emplean tecnologías avanzadas, particularmente sistemas de armas autónomos, capaces de identificar, seleccionar y atacar objetivos sin intervención humana directa durante la operación. Estos sistemas, impulsados por inteligencia artificial y sensores, permiten a las fuerzas*

*militares realizar ataques con una mínima supervisión humana, aunque en algunos casos pueden existir mecanismos de anulación por parte de los operadores.*

Del mismo modo, es relevante señalar que la *guerra autónoma* plantea desafíos éticos y legales considerables, ya que delegar en las máquinas decisiones de vida o muerte puede socavar los principios del derecho internacional humanitario y aumentar el riesgo de daño colateral, especialmente en la protección de civiles. A nivel técnico, estos sistemas varían en su nivel de autonomía, desde funciones automáticas simples hasta la toma de decisiones casi completa sin interacción humana, lo que ha suscitado debates en la comunidad internacional sobre la necesidad de su regulación.

### **Sistemas de armas autónomos letales y algunos ejemplos**

Los LAWS, tal como los entiende el CICR, son cualquier arma que seleccione y aplique fuerza a objetivos sin intervención humana. Una persona activa un arma autónoma, pero desconoce quién será el objetivo y cuándo ocurrirá el ataque, ni exactamente dónde y/o cuándo se producirá ese ataque. Esto se debe a que un arma autónoma se activa mediante sensores y software, que comparan lo que los sensores detectan en el entorno con un *perfil de objetivo* (Davison, 2022). Un ejemplo de esto, podría ser la forma de un vehículo militar o el movimiento de una persona. Es el vehículo o la víctima el que desencadena el ataque, no el usuario. En ese sentido, la preocupación en torno a este proceso radica en la ausencia de criterio humano con relación al uso de la fuerza, la cual claramente dificulta el control sobre los efectos de estas armas.

En ese sentido, es relevante destacar que en los últimos años con el crecimiento de la IA estos sistemas de armas han evolucionado de manera exponencial ya que pueden identificar, seleccionar y eliminar objetivos sin la intervención humana, lo cual hace que estos sistemas sean una preocupación de importantes centros de estudio a nivel mundial.

### **Algunos ejemplos de LAWS**

#### *Vision 60 Q-UGV*

El VISION 60 Q-UGV es un robot cuadrúpedo autónomo diseñado y desarrollado por la empresa Ghost Robotics para misiones de reconocimiento, vigilancia y seguridad (ver figura N°1). Este vehículo terrestre no tripulado (UGV, por sus siglas en inglés) se destaca por su capacidad para operar en una amplia variedad de terrenos, desde zonas urbanas hasta entornos más hostiles, gracias a su diseño robusto y su capacidad para caminar, correr y navegar en terrenos irregulares. Es

completamente autónomo y puede ser programado para realizar patrullas predefinidas, detectar y evitar obstáculos, y llevar a cabo tareas de monitoreo sin intervención humana constante.

Uno de los aspectos más innovadores es su capacidad para integrarse con diferentes tipos de sensores y cargas útiles, como cámaras térmicas, dispositivos de comunicación o incluso armamento no letal. Además, su autonomía le permite operar en entornos donde el acceso humano es peligroso o difícil, proporcionando inteligencia en tiempo real sin arriesgar la vida humana. El uso de este UGV ha sido explorado en varios contextos, incluidos despliegues militares y tareas de seguridad civil, lo que demuestra el creciente papel de los robots cuadrúpedos en el campo de la seguridad y defensa (Army Technology, 2022).

**Figura N° 1**  
*Vision 60 Q-UGC*



*Nota:* Tomada del sitio web [army-technology.com](https://www.army-technology.com/projects/ghost-robotics-v60-unmanned-ground-vehicle-usa/?cf-view) de fecha 22 de septiembre de 2024 desde <https://www.army-technology.com/projects/ghost-robotics-v60-unmanned-ground-vehicle-usa/?cf-view>

### *Drone naval Magura V5*

En el ámbito naval, uno de los LAWS que más han llamado la atención a especialistas en defensa son los enjambres de drones autónomos que atacaron la flota naval rusa en el Mar Negro, en el marco del conflicto entre Rusia y Ucrania (octubre 2023 en Sebastopol). Estos drones, diseñados específicamente para realizar misiones de combate sin intervención humana directa durante la operación,

utilizaron sensores avanzados y algoritmos de IA para identificar los buques de guerra rusos, y proceder al ataque.

Una vez activados, maniobraron y atacaron por sí mismos, en áreas donde las comunicaciones con los operadores humanos eran limitadas o imposibles. Además de su capacidad para operar sin supervisión directa, estos drones pueden coordinarse entre sí de manera autónoma y ejecutar ataques en enjambre complicando de esta forma a las defensas tradicionales de la flota, maximizando el impacto del ataque y reduciendo las posibilidades de interceptación (US Naval Institute, 2022).

## **Figura N° 2**

*Drone naval Magura V5*



*Nota:* Tomada del sitio web [news.usni.org](https://news.usni.org/2022/10/11/suspected-ukrainian-explosive-sea-drone-made-from-jet-ski-parts) de fecha 10 de septiembre de 2024 desde <https://news.usni.org/2022/10/11/suspected-ukrainian-explosive-sea-drone-made-from-jet-ski-parts>

## *Dron kamikaze Shahed 136*

El Shahed 136 es un dron kamikaze desarrollado por Irán que ha ganado notoriedad por su uso en el conflicto entre Rusia y Ucrania (ver figura N°3). Se trata de una munición merodeadora diseñada para ataques de largo alcance, capaz de identificar y lanzarse contra su objetivo, explotando en el impacto. Este dron puede volar de manera completamente autónoma, gracias a su sistema de navegación por GPS, lo que le permite cubrir distancias de hasta 2.500 km sin intervención humana una vez

lanzado. Su capacidad de vuelo autónomo le permite operar en enjambres, saturando las defensas aéreas del enemigo lo que lo hace difícil de interceptar. Su costo relativamente bajo y su facilidad de producción lo han convertido en un arma crucial en la guerra moderna, siendo utilizado principalmente para atacar infraestructuras críticas y militares. El Shahed 136 ha demostrado ser una herramienta eficaz en conflictos asimétricos, al proporcionar a los usuarios la capacidad de realizar ataques precisos a gran distancia sin arriesgar tripulaciones humanas (Rojas, 2024).

### **Figura N° 3**

*Dron kamikaze Shahed 136*



*Nota:* Tomada de edición digital del diario La Razón de fecha 12 de septiembre de 2022 desde <https://www.larazon.es/tecnologia/20221010/p56dfllscfcexo65cecvz46soy.html>

### *Drone kamikaze Lanius*

Elbit Systems, dentro de su programa Legión X, creó el año 2022 el dron *Lanius* (ver figura N°4), definido como una munición merodeadora basada en drones altamente maniobrables y versátiles, diseñada para operaciones de corto alcance en el entorno urbano capaz de explorar y mapear de manera autónoma edificios y puntos de interés en busca de posibles amenazas (Elbit Systems, 2024). Llamado así por una especie de ave similar a los gorriones, las capacidades de este pequeño aparato de solo 1,25 kilos son temibles para el enemigo: alcanza los 70 km/h de

vuelo autónomo y transporta una carga explosiva de hasta 150 gramos. Se usa para operaciones a ras de suelo o incluso dentro de edificios. Entre sus múltiples posibilidades, es capaz de localizar y atacar objetivos específicos basados en IA actuando como drones kamikazes. Otro aspecto relevante es que su diseño fue pensado como una solución de combate de red autónoma de múltiples dominios capaz de generar enjambres heterogéneos no tripulados que comparten información y son capaces de atacar en forma coordinada (Elbit Systems, 2024).

#### **Figura N° 4**

*Drone kamikaze Lanius*



*Nota:* Tomada del sitio web Elbit Systems de fecha 7 de septiembre de 2024 desde <https://elbitsystems.com/product/lanius/>.

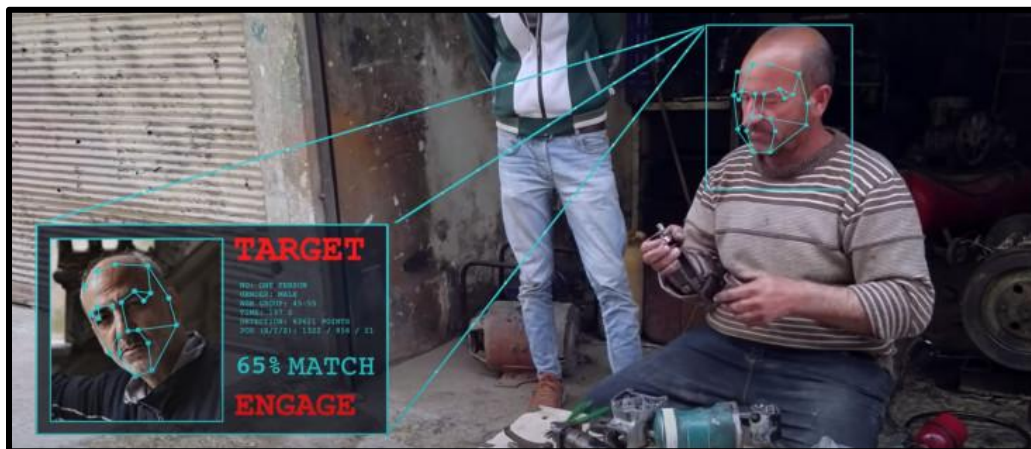
#### *Software para adquisición de objetivos Lavender*

El software Lavender, utilizado por las Fuerzas de Defensa de Israel, es una plataforma de inteligencia artificial diseñada para optimizar las operaciones militares en la Franja de Gaza. Este sistema emplea bases de datos masivas y realiza análisis avanzados en tiempo real para identificar objetivos relacionados con Hamás y otros grupos militantes, facilitando los ataques aéreos de precisión. Al reducir el tiempo de reacción y mejorar la exactitud de los ataques, Lavender representa un salto tecnológico significativo en el uso de sistemas autónomos en el campo de batalla,

pero también ha suscitado preocupaciones éticas sobre la automatización de decisiones bélicas y el potencial aumento de daños colaterales.

### **Figura N° 5**

*Software para adquisición de objetivos Lavender*



*Nota:* Tomada del sitio web del Comité Internacional de la Cruz Roja de fecha 7 de septiembre de 2024 desde <https://www.icrc.org/es/document/preguntas-y-respuestas-sobre-armas-autonomas>

### **Argumentos a favor de los sistemas de armas autónomos letales**

En la comunidad de defensa internacional, el apoyo para el empleo de LAWS, se basa principalmente en las ventajas militares que estos pueden aportar y en las justificaciones morales para su uso.

Con respecto a las primeras de ellas, una de las principales ventajas es que los LAWS pueden actuar como multiplicadores de fuerza, ya que, la eficacia de cada combatiente es mayor, además de necesitar menos combatientes (soldados) para la misión encomendada. De la misma forma, los LAWS tienen la capacidad de alcanzar zonas donde al humano no le es posible llegar, ya sea, por las condiciones adversas del terreno, la inclemencia del tiempo atmosférico o por lo nocivo del ambiente ante situaciones químicas, bacteriológicas, radiológicas y nucleares (CBRN en inglés), ampliando claramente el campo de batalla. Por último, los sistemas de armas autónomos pueden reducir las bajas al reemplazar a los combatientes soldados de misiones peligrosas (Marchant, 2021).

Así también, se ha enfatizado en la posibilidad de ahorrar dinero a largo plazo mediante la utilización de una fuerza de robots. En un artículo de 2013 publicado en *The Fiscal Times* indica que cada soldado en Afganistán le costaba al Pentágono aproximadamente 850.000 dólares por año, en cambio, el Oshkosh RCV, un

vehículo de combate robótico (RCV, en inglés) equipado con una estación de armas remota Kongsberg RS6, un módulo de oscurecimiento de humo L3, un cañón LW de 30x113 mm y un sistema lanzador de municiones merodeadoras/UAS Switchblade 300 de AeroVironment, podría costar 480.000 dólares por año (Quinetiq, 2024).

**Figura N° 6**  
*Oshkosh RCV*



Nota: Tomada del sitio web de la empresa Qinetiq el 10 de septiembre de 2024 desde <https://oshkoshdefense.com/vehicles/combat-vehicles/rcv/>

Otro aspecto importante que considerar es que gracias a la IA es que los LAWS tienen el potencial único de operar a un ritmo mucho más rápido y sostenido, ya que, no están propensos a las limitaciones fisiológicas y mentales que los humanos tienen, pero lo más destacable es la habilidad para atacar letalmente, incluso, cuando se han cortado los vínculos de comunicación (Thurnher, 2016).

Por último, es relevante destacar lo señalado en un informe de la Junta de Ciencias de la Defensa de EE.UU. de 2012, en el que se identifican seis áreas claves en las que los avances en autonomía tendrían un beneficio significativo para un LAWS: *percepción, planificación, aprendizaje, interacción humano-robot, comprensión del lenguaje natural y coordinación multiagente* (Defense Science Board, 2012, p. 31).

Veamos ahora cómo fueron definidas las seis áreas claves por dicha Junta. Con respecto a la *percepción*, se refiere a los sensores y la detección, donde los sensores están hechos de hardware, y la detección está hecha de software, lo cual, en su conjunto permite la obtención de información para una posterior acción (Defense Science Board, 2012, pág. 33). La *planificación* se refiere a “calcular una secuencia o una orden parcial de acciones que logren un estado deseado” (Defense Science Board, 2012, pág. 38). Esta secuencia se basa en procesos efectivos y “algoritmos necesarios para tomar decisiones sobre acciones (proporcionar autonomía) en situaciones en las que los humanos no están en el entorno (por ejemplo, el espacio, el océano)” (Defense Science Board, 2012, págs. 38-39).

Luego, *el aprendizaje* se refiere a cómo las máquinas pueden recopilar y procesar grandes cantidades de datos para convertirlos en conocimiento. El informe afirma que la investigación ha demostrado que las máquinas procesan los datos para convertirlos en conocimiento con mayor eficacia que las personas (Defense Science Board, 2012, pág. 41). *La interacción entre humanos y robots* se refiere a “cómo las personas trabajan o juegan con los robots” (Defense Science Board, 2012, pág. 44). Los robots son bastante diferentes de otras computadoras o herramientas porque son “agentes situados físicamente” y los usuarios humanos interactúan con ellos de maneras distintas (Defense Science Board, 2012, pág. 44).

*El procesamiento del lenguaje natural* se refiere a “sistemas que pueden comunicarse con personas usando lenguajes humanos comunes” (Defense Science Board, 2012, pág. 49). Además, “el lenguaje natural es la forma más normal e intuitiva que tienen los humanos de dar instrucciones a los sistemas autónomos; les permite proporcionar diversos objetivos y estrategias de alto nivel en lugar de una tele operación detallada”. Por lo tanto, es necesario un mayor desarrollo de la capacidad de los sistemas de armas autónomas para responder a comandos en un lenguaje natural (Defense Science Board, 2012, pág. 49).

Finalmente, el Consejo Científico de Defensa emplea la expresión coordinación multi agente para situaciones en las que una tarea se distribuye entre “varios robots, agentes de software o humanos” (Defense Science Board, 2012, pág. 50). Las interacciones de los agentes pueden ayudar a planificar o a coordinar las tareas de forma centralizada debido a que “supone que los agentes tienen una comprensión cognitiva de las capacidades de los demás, pueden supervisar el progreso hacia el objetivo y participar en un trabajo en equipo más parecido al de los humanos”, este tipo de coordinación va más allá de la mera cooperación (Defense Science Board, 2012, pág. 50).

Con respecto a las justificaciones morales, varios especialistas en ética y tecnología han argumentado que los LAWS pueden ser moralmente aceptables debido a su capacidad de operar sin las limitaciones humanas, como el miedo o el cansancio. Según Vincent Müller (2021), las máquinas podrían tomar decisiones en combate de manera más ética que los humanos, ya que no estarían influenciadas por emociones o sesgos personales. Müller sostiene que la programación de estos sistemas con códigos morales predefinidos permitiría evitar acciones impulsivas o excesivas, reduciendo así el riesgo de violaciones al derecho internacional humanitario. A diferencia de los soldados humanos, los LAWS no actúan bajo instintos de supervivencia, lo que podría evitar comportamientos reactivos como el “dispara primero, pregunta después” (Müller, 2021).

Las decisiones que tomen los LAWS no estarán condicionados por emociones humanas como el miedo o la histeria, lo que les permitiría procesar grandes cantidades de información sin distorsionar los datos sensoriales para ajustarse a sesgos preconcebidos. Según un análisis de Matti Häyry (2021), en un contexto militar, los LAWS podrían ser más confiables a la hora de reportar infracciones éticas en comparación con los soldados humanos, quienes podrían verse influidos por la presión social del grupo. Häyry destaca que, mientras los robots actúan bajo una programación estricta que sigue principios éticos, los humanos en un equipo militar pueden cerrar filas para encubrir malas prácticas, algo que los LAWS evitarían al no estar sujetos a este tipo de dinámicas de grupo (Häyry, 2021).

### **Argumentos en contra de los sistemas de armas autónomos letales**

La principal oposición para el uso de los LAWS se encuentra en razones éticas, no obstante, es importante señalar que estos argumentos morales podrían ser erróneos y que la comunidad internacional se encuentra dividida ante este dilema. La oposición por razones éticas. En una conferencia conjunta internacional sobre la inteligencia artificial en julio de 2015, se publicó una carta abierta que exigía la prohibición de los LAWS. En la misiva se destaca que la tecnología de IA ha llegado a un punto en el que la implementación de estos sistemas será prácticamente factible en unos años, no décadas, aunque con altos riesgos. Las armas autónomas han sido descritas como la tercera revolución en la guerra, después de la pólvora y las armas nucleares (Artificial Intelligence & Robotics Researchers, 2015).

Esta carta también menciona que, aunque la IA tiene el potencial de ayudar a la humanidad, una carrera armamentística con IA militar podría dañar su reputación y generar una reacción pública negativa reduciendo sus futuros beneficios. La misiva cuenta con una gran cantidad de signatarios, incluyendo al inventor y fundador de Tesla, Elon Musk, Steve Wozniak (cofundador de Apple), el físico Stephen Hawking

(de la Universidad de Cambridge) y Noam Chomsky (del Instituto de Tecnología de Massachusetts). Además, la mencionada carta fue firmada por más de 3000 expertos en robótica e inteligencia artificial, los cuales abiertamente exigen la prohibición de armas ofensivas independientes del control humano (Artificial Intelligence & Robotics Researchers, 2015).

Si bien la carta menciona armas ofensivas, es importante señalar que a veces no es posible determinar si un arma es ofensiva o defensiva. Ejemplo de esta ambigüedad puede ser el uso de drones armados. Si bien estos vehículos no tripulados pueden usarse para vigilancia y defensa, su capacidad para llevar a cabo ataques preventivos en territorios enemigos también los convierte en una herramienta ofensiva. Esto puede generar tensiones significativas ya que, una nación que posea drones avanzados podría ser percibida como una amenaza constante, capaz de intervenir sin advertencia en conflictos fuera de su territorio.

En el año 2013, un grupo de ingenieros, especialistas en IA y tecnología mecánica, y otros investigadores y analistas de treinta y siete países emitieron el *Llamado de los científicos para boicotear los LAWS*. El documento señala la necesidad de una prueba lógica de que los robots pueden, en el futuro, tener “la utilidad requerida para una prueba precisa de distinción de objetivos, atención situacional o decisiones con respecto al uso relativo de la fuerza” (International Committee for Robot Arms Control, 2013), de lo contrario estos podrían causar un gran nivel de daño colateral. Finalmente, el documento concluye exigiendo que “las decisiones sobre la aplicación de la violencia no deben asignarse a las máquinas” (International Committee for Robot Arms Control, 2013).

Confiar a sistemas autónomos la decisión respecto a la vida o muerte plantea serias preocupaciones éticas y legales. En ese sentido, el principal problema radica en la incapacidad que tienen los LAWS para cumplir con los principios del derecho internacional humanitario, como la distinción y la proporcionalidad, lo que podría resultar en una mayor cantidad de víctimas civiles. A su vez, Stuart Russell, destacado experto en IA, señala que la delegación de estas decisiones a máquinas despoja a los seres humanos de la responsabilidad moral y abre la puerta a la deshumanización del conflicto armado. Este enfoque podría exacerbar los daños colaterales y generar consecuencias catastróficas para la seguridad global, ya que los algoritmos carecen de la empatía y el juicio necesarios para tomar decisiones éticas en entornos de combate complejos (Russell, 2019).

La cuestión de la rendición de cuentas en el uso de LAWS también es una preocupación crítica en el ámbito del derecho internacional. Según Peter Asaro, un reconocido académico en ética de la IA, los LAWS plantean serios desafíos en

cuanto a la asignación de responsabilidad, ya que las decisiones de vida o muerte son tomadas por algoritmos y no por humanos, lo que complica la capacidad para responsabilizar a un individuo o entidad por posibles violaciones del derecho humanitario. Asaro advierte que, en ausencia de una figura clara responsable de las acciones de estas máquinas, el principio del *jus in bello* se ve erosionado, lo que socava la legitimidad de los mecanismos de justicia y rendición de cuentas en los conflictos armados (Asaro, 2016).

Este problema se origina en el hecho de que las computadoras equipadas con IA toman decisiones por sí mismas; por lo tanto, es difícil identificar la fuente de una decisión errónea, ya sean errores programáticos o la toma de decisiones autónoma de las máquinas equipadas con IA (las llamadas inteligentes). La naturaleza de este problema salió a la luz cuando un vehículo autónomo conducía demasiado rápido en una autopista, excediendo el límite de velocidad indicado, y no estaba claro quién debía recibir la multa (Etzioni & Etzioni, 2016).

La regulación de los LAWS ha generado intensos debates entre académicos y expertos en derecho internacional. Según Brundage et al. (2020), es fundamental que los marcos regulatorios se desarrollen simultáneamente con el avance de la tecnología para evitar que los sistemas de armas autónomos escapen al control humano. Este enfoque proactivo busca crear sistemas con *alineación de valores*, donde los algoritmos no solo sigan reglas estrictas, sino que también sean capaces de adaptar su comportamiento en base a principios éticos universales. Además, los autores advierten que el retraso en la regulación podría conducir a graves consecuencias éticas, como la imposibilidad de responsabilizar a los desarrolladores o usuarios de estos sistemas por decisiones moralmente cuestionables (Brundage, Avin, Wang, Hadfield, & Dafoe, 2020).

Finalmente, Anderson y Waxman, señalan que los humanos probablemente se aclimatarán a la integración de la tecnología de IA en las armas a medida que se acostumbren a que las computadoras realicen tareas cotidianas y aquellas que tienen repercusiones de muerte, como operar maquinaria o realizar una cirugía. Por lo tanto, los autores antes mencionados sugieren que el mundo se debe centrar en crear normas y principios (en lugar de regulaciones legalmente vinculantes) que guiarán y limitarán el desarrollo, la investigación y el eventual despliegue de LAWS (Anderson & Waxman, 2013). Lo anterior, podría ayudar a establecer expectativas de comportamiento que sean moral o legalmente aceptables por los humanos para que las máquinas puedan operar en los campos de batalla actuales.

## Conclusiones

El desarrollo y la implementación de los LAWS en los últimos años nos ha llevado a un punto crítico en la historia de la guerra moderna. Lo que antes se concebía como una ficción distópica en películas como *Terminator* hoy está más cerca de convertirse en una realidad cotidiana en los campos de batalla, con drones y sistemas autónomos que toman decisiones letales de manera independiente. La evolución de estas tecnologías, como el software *Lavender* y los drones como el *Shahed 136*, *Magura V5* y *Lanius*, han transformado la manera como se libran los conflictos, llevando la guerra a una nueva dimensión donde el papel del ser humano en el combate está cada vez más diluido.

El uso de LAWS plantea serios desafíos éticos y legales. La capacidad de estas máquinas para operar sin supervisión humana no solo abre la puerta a conflictos más automatizados, sino que también, introduce preguntas difíciles sobre la rendición de cuentas y la responsabilidad en caso de fallos o daños colaterales. ¿Quién es responsable cuando una máquina, sin intervención humana, toma una decisión errónea que resulta en la pérdida de vidas civiles? La posibilidad de que los LAWS operen sin la supervisión humana adecuada no solo deshumaniza la guerra, sino que también, complica la aplicación del derecho internacional humanitario, que se basa en la toma de decisiones humanas en contextos complejos.

A pesar de los avances tecnológicos, también es esencial reconocer que estas armas no son infalibles. La dependencia en la inteligencia artificial y los algoritmos implica un riesgo inherente de errores o fallos imprevistos, especialmente en entornos de combate caóticos y en evolución. Además, la posibilidad que estas tecnologías sean utilizadas por actores no estatales o en situaciones de conflicto no reguladas añade una capa de incertidumbre que la comunidad internacional aún debe abordar. El despliegue de drones autónomos en la guerra entre Rusia y Ucrania y en el conflicto entre Israel y Hamas es solo una muestra de los peligros que podrían escalar en futuros enfrentamientos.

Finalmente, la *guerra autónoma* marca un cambio paradigmático en la forma como entendemos los conflictos armados, pero también exige una reevaluación profunda de los marcos éticos, legales y humanitarios que deben regir su uso. Es importante que las naciones y las organizaciones internacionales colaboren para establecer regulaciones claras que aseguren que el uso de estas tecnologías no comprometa los valores fundamentales de la humanidad. A medida que avanzamos hacia un futuro donde las máquinas juegan un papel cada vez más central en la guerra, la responsabilidad de garantizar que estas innovaciones se utilicen de manera ética y

controlada recae en todos. El desafío no es solo tecnológico, sino moral: asegurar que la autonomía de las máquinas no signifique la pérdida de control humano sobre la vida y la muerte.

### **ACRÓNIMOS Y SIGLAS**

|      |                                                |
|------|------------------------------------------------|
| CBRN | Chemical, Biological, Radiological and Nuclear |
| CICR | Comité Internacional de la Cruz Roja           |
| CSIS | Center for Strategic and International Studies |
| GPS  | Global Position System                         |
| IA   | Inteligencia Artificial                        |
| LAWS | Lethal Autonomous Weapons Systems              |
| ONU  | Organización de Naciones Unidas                |
| RCV  | Robotic Combat Vehicle                         |
| UGV  | Unmanned Ground Vehicle                        |

## Referencias

- Anderson, K., & Waxman, M. C. (2013). *Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can*. Jean Perkins Task Force on National Security and Law Essay Series, 34.
- Army Technology. (20 de septiembre de 2022). *Army Technology*. Obtenido de Army-technology.com: <https://www.army-technology.com/projects/ghost-robotics-v60-unmanned-ground-vehicle-usa/?cf-view>
- Artificial Intelligence & Robotics Researchers. (28 de Julio de 2015). Obtenido de Future of Life Institute: <http://futureoflife.org/open-letter-autonomous-weapons/>.
- Asaro, P. (2016). *Jus nascendi, robotic weapons and the Martens Clause*. En N. Bhuta, S. Beck, R. Geib, H.-Y. Liu, & C. Krebs, *Autonomous Weapons Systems: Law, Ethics, Policy* (págs. 121-140). Cambridge: Cambridge University Press.
- Brundage, M., Avin, S., Wang, J., Hadfield, G., & Dafoe, A. (2020). *oward trustworthy AI development: Mechanisms for supporting verifiable claims*. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency.
- Center for Strategic and International Studies. (6 de Enero de 2022). *CSIS*. Obtenido de *DOD is updating its decade-old autonomous weapons policy, but confusion remains widespread*: <https://www.csis.org/analysis/dod-updating-its-decade-old-autonomous-weapons-policy>
- Comité Internacional de la Cruz Roja. (26 de Julio de 2022). *CICR*. Obtenido de *What you need to know about autonomous weapons*: <https://www.icrc.org/en/document/what-you-need-know-about-autonomous-weapons>
- Davison, N. (22 de Julio de 2022). Obtenido de [icrc.org: https://www.icrc.org/es/document/preguntas-y-respuestas-sobre-armas-autonomas](https://www.icrc.org/es/document/preguntas-y-respuestas-sobre-armas-autonomas)
- Defense Science Board. (2012). *The Role of Autonomy in DoD Systems*. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.
- Elbit Systems. (7 de septiembre de 2024). Obtenido de Elbit Systems: <https://elbitsystems.com/product/lanius/>
- Etzioni, A., & Etzioni, O. (2016). *Keeping AI Legal*. *Vanderbilt Journal of Entertainment & Technology Law*, 133-146.

- Häyry, M. (2021). *Employing Lethal Autonomous Weapon Systems: Ethical Issues in the Use of Artificial Intelligence in Military Leadership*. *International Journal of Applied Philosophy*.
- Marchant, G. E. (2021). *International Governance of Autonomous Military Robots*. *Columbia Science and Technology Law Review* (12), 272-276.
- Müller, V. (2021). *Ethics of Artificial Intelligence*. En A. Elliott, *The Routledge Social Science Handbook of AI* (págs. 122-137). Londres: Routledge .
- Naciones Unidas. (22 de septiembre de 2023). *Naciones Unidas*. Obtenido de Explainer: *What is international humanitarian law?* UN News: <https://news.un.org/en/story/2023/09/explainer-international-humanitarian-law>.
- Quinetiq. (9 de septiembre de 2024). *Quinetiq*. Obtenido de Quinetiq.com: <https://www.qinetiq.com/en/what-we-do/services-and-products/rcv-l>
- Rojas, A. (13 de abril de 2024). *El Mundo*. Obtenido de elmundo.es: <https://www.elmundo.es/internacional/2024/04/13/661af9bbfc6c83996a8b4591.html>
- Russell, S. (2019). *Human Compatible: Artificial Intelligence and the Problem of Control*. Nueva York: Viking.
- The University of Queensland. (8 de diciembre de 2021). *uq.edu.au*. Obtenido de Autonomous weapon systems: Law and the future of war.: <https://law.uq.edu.au/research/law-and-future-war>
- Thurnher, J. S. (2016). Legal Implications of Fully Autonomous Targeting. *Joint Force Quarterly* (67), 83.
- US Naval Institute. (11 de octubre de 2022). *US Naval Institute*. Obtenido de news.usni.org: <https://news.usni.org/2022/10/11/suspected-ukrainian-explosive-sea-drone-made-from-jet-ski-parts>



# LA IMPORTANCIA DEL APOYO LOGÍSTICO ANTICIPADO EN EL ÉXITO DE LAS OPERACIONES DE PAZ

*The importance of anticipated logistical support in the success of peace operations*

May. Esteban Vásquez Mulsow<sup>1</sup>

## Resumen

El artículo analiza la importancia del apoyo logístico anticipado para el éxito de las operaciones de paz, especialmente en contextos donde la infraestructura del país anfitrión ha sido gravemente dañada. Se sostiene que la planificación logística proactiva es fundamental para asegurar una respuesta efectiva ante las emergencias que enfrentan las fuerzas desplegadas por la ONU. A través de una revisión de mejores prácticas, se resalta cómo una logística bien estructurada optimiza el uso de los recursos y refuerza la capacidad de las misiones de paz para cumplir con su mandato, contribuyendo así a crear un entorno seguro y facilitando la efectividad operativa y promoviendo así un ambiente estable y seguro en situaciones de conflicto.

**Palabras clave** Apoyo logístico anticipado - Operaciones de paz - Planificación proactiva - Efectividad operativa.

## Abstract:

The article discusses the importance of anticipated logistical support for the success of peace operations, especially in contexts where the host country's infrastructure has been severely damaged. It is argued that proactive logistics planning is essential to ensure an effective response to emergencies faced by the forces deployed by the UN. Through a review of best practices, it highlights how well-structured logistics optimize the use of resources and strengthen the capacity of peace missions to fulfill their mandate, thus contributing to creating a secure environment and facilitating operational effectiveness and thus promoting a stable and safe environment in conflict situations.

**Keywords:** Anticipated logistical support - Peace operations - Proactive planning - Operational effectiveness.

---

<sup>1</sup> Oficial de Estado Mayor del Servicio de Intendencia. Especialista en Instrucción Militar de Montaña, Paracaidista Básico Militar y Profesor de Academia en Logística. Actualmente se desempeña como Comandante del Batallón de Alumnos de la Escuela de los Servicios de Ejército de Chile. Correo electrónico: [esteban.vasquez@ejercito.cl](mailto:esteban.vasquez@ejercito.cl)

## Introducción

Las operaciones de paz de las Naciones Unidas se clasifican en cinco tipos principales:

- **Prevención de conflictos:** Se enfoca en evitar el estallido de conflictos mediante herramientas como la mediación, la diplomacia preventiva y la promoción de confianza entre las partes. Es una estrategia proactiva para abordar tensiones antes de que escalen.
- **Mantenimiento de la paz:** Incluye el despliegue de personal militar, policial y civil para estabilizar situaciones, proteger civiles y garantizar el cumplimiento de acuerdos de paz. Estas misiones requieren el consentimiento de las partes involucradas, la imparcialidad y el uso mínimo de la fuerza, excepto en defensa del mandato.
- **Consolidación de la paz:** Tiene como objetivo ayudar a los países en la recuperación postconflicto, fortaleciendo instituciones y promoviendo el desarrollo sostenible para prevenir la reaparición de conflictos.
- **Imposición de la paz:** Son operaciones con mandatos más robustos, que pueden autorizar el uso de la fuerza para proteger civiles o garantizar el cumplimiento de resoluciones del Consejo de Seguridad. Se aplican en situaciones inestables o donde las partes no cooperan plenamente.
- **Asistencia humanitaria:** Aunque no siempre se consideran operaciones de paz formales, muchas misiones integran componentes humanitarios para atender necesidades inmediatas, como el suministro de alimentos y la protección de refugiados y desplazados.

La logística anticipada es crucial para la efectividad de las Operaciones de Paz (OPAZ) detalladas en el párrafo anterior, las cuales corresponden a actividades desarrolladas por la ONU para mantener o restablecer la paz y la seguridad internacionales en escenarios de conflicto o postconflicto, siendo aprobadas mediante mandatos específicos del Consejo de Seguridad o la Asamblea General de la ONU, implicando el despliegue de personal militar, policial y/o civil. Al respecto, una planificación logística que prevea y satisfaga con precisión las necesidades de la misión resulta esencial, ya que permite una respuesta rápida y eficaz en entornos complejos e impredecibles, como aquellos afectados por infraestructuras devastadas. Este enfoque garantiza que las fuerzas desplegadas puedan cumplir con éxito su mandato y adaptarse a los desafíos sobre el terreno.

En relación a lo anterior, la función logística se presenta como uno de los pilares fundamentales del éxito en estas operaciones; con el tiempo, las misiones de mantenimiento de la paz de la ONU han requerido un enfoque coordinado y complejo para afrontar los desafíos en el terreno; en cuanto a esto, en entornos volátiles donde la infraestructura del país anfitrión es limitada, la logística anticipada adquiere un valor estratégico, facilitando la movilización ágil de recursos y la implementación de acciones críticas necesarias para el cumplimiento del mandato.

La planificación logística anticipada no solo tiene como objetivo abastecer a los contingentes desplegados, sino también garantizar que las fuerzas puedan operar con eficiencia en circunstancias difíciles. Como señala Rod Little<sup>2</sup> (2018) “No se podrá implementar con éxito el mandato sin coordinación a nivel operativo y logístico”. (p.139). Este enfoque permite que las OPAZ se ejecuten con rapidez, precisión y, sobre todo, con la capacidad de responder a las necesidades emergentes sin dilaciones que puedan poner en riesgo a la misión o a la población civil.

Una de las principales características de la logística en OPAZ es su capacidad para adaptarse a entornos heterogéneos, donde participan actores tan diversos como militares, civiles, policías y observadores internacionales. Cada uno de estos componentes requiere un apoyo logístico específico y oportuno para desempeñar sus tareas de manera eficaz. Para lograr un despliegue eficiente y sostenible en OPAZ, será esencial que la planificación logística se base en un entendimiento claro del contexto geopolítico, y de las condiciones del terreno y desafíos logísticos preexistentes.

La aplicación de un enfoque de logística anticipada, por tanto, no solo aumenta la capacidad de respuesta de las fuerzas desplegadas, sino que también minimiza las interrupciones que puedan derivarse de la falta de recursos o planificación. Como menciona la carta de las Naciones Unidas: “el Consejo de Seguridad tiene como principal responsabilidad la paz y la seguridad internacionales. Es en este entorno que la logística juega un rol vital” (p.14).

---

<sup>2</sup> El Mayor (R.) Rod Little es un Oficial de Logística de las Fuerzas Armadas de Canadá, con una distinguida trayectoria en la gestión logística militar. Se retiró como G4 de la 36ª Brigada, siendo responsable del transporte, mantenimiento y suministro de las unidades del Ejército en Nueva Escocia y la Isla Príncipe Eduardo. A lo largo de su carrera, ha liderado operaciones clave, entre ellas su participación en el Centro Internacional de Capacitación de Apoyo para la Paz en Nairobi, Kenia, donde completó múltiples cursos de logística de Naciones Unidas y desempeñó un rol de liderazgo en la capacitación de personal militar y civil internacional.

Al respecto, el apoyo logístico en las OPAZ es un factor relevante para su éxito; las misiones de mantenimiento de la paz de la ONU han evolucionado para adaptarse a diversas tareas que promueven la paz y la seguridad en entornos complejos. En estos escenarios, la infraestructura del país anfitrión suele ser limitada o gravemente afectada, lo que resalta la necesidad de una logística eficiente y anticipada; así, la logística en estas operaciones enfrentará desafíos únicos debido a la diversidad de actores involucrados<sup>3</sup>, cada uno con necesidades específicas que requieren una planificación detallada. En este contexto, la logística anticipada es clave para permitir la rápida movilización de recursos y una respuesta ágil a las demandas del mandato de la misión.

Como señala Bovey<sup>4</sup> et al (2015): “la movilidad y la agilidad de una fuerza son claves para operar en territorios donde no hay una infraestructura real” (Bovey, 2015, como se cita en Cruz, 2019 p.15); esta capacidad para prever los requerimientos permite que las fuerzas no solo lleguen rápidamente a su destino, sino que se mantengan operativas en el terreno durante el tiempo necesario, por lo tanto, la coordinación anticipada de suministros<sup>5</sup>, es importante para adaptarse a las condiciones de cada zona. Un ejemplo de logística anticipada fue el despliegue en la crisis de Darfur, donde la ONU subrayó la importancia de contar con una estructura logística preparada para enfrentar las dificultades de las rutas y la falta de infraestructura, permitiendo una instalación rápida y efectiva de las fuerzas, asegurando el cumplimiento de los objetivos estratégicos y minimizando los riesgos para los efectivos y la población civil.

En este sentido, el aporte de la logística anticipada reside en la previsión de los desafíos inherentes a cada misión; esta capacidad de adelantarse a las necesidades operativas facilita la adaptabilidad y efectividad del contingente, asegurando que las fuerzas puedan concentrarse en sus tareas primarias, como la protección de civiles, sin preocuparse de la falta de recursos esenciales. En consecuencia, el objetivo de este artículo es analizar como la planificación proactiva y la logística anticipada no solo optimizarán los recursos, sino que serán claves para el éxito en las OPAZ, al ser un pilar estratégico, impactando directamente en la efectividad de las misiones y la protección de las poblaciones en riesgo.

---

<sup>3</sup> Contingentes militares, personal civil y fuerzas policiales.

<sup>4</sup> Bovey, Vincenzo; Ruggeri, Andrea. Kinds of Blue: Diversity in U.N. Peacekeeping Missions and Civilian Protection. *British Journal of Political Science*, 2015, 1-20 (9).

<sup>5</sup> Equipos, medicinas, víveres y otros insumos.

## Algunos antecedentes históricos

Tras la Segunda Guerra Mundial, 51 países fundaron la ONU con el objetivo de proteger a futuras generaciones de la guerra, promoviendo actividades orientadas a la paz y la seguridad (ONU, 2024). Entre estas, destacan las operaciones de mantenimiento de la paz, gestionadas por el Departamento de OPAZ de la ONU, que buscan implementar acuerdos de paz y evitar recaídas en la violencia en países en conflicto.

Chile, desde 1945, ha respaldado la Carta de la ONU como base jurídica para la seguridad internacional. Participa activamente en misiones de paz desde 1948, comenzando con observadores militares en Medio Oriente. Con el tiempo, la ONU ha adaptado sus operaciones para incluir fuerzas militares, policiales y civiles, contribuyendo a la estabilidad de los países anfitriones. A principios del 2000, Chile aumentó su participación en las OPAZ, organizando sus tropas y personal para cumplir con las normativas de la ONU, asesorar a sus autoridades y asegurar una preparación adecuada para estas misiones.

Al respecto, “El 15 de julio de 2002, mediante el Decreto Supremo MDN.SSG.DEPTO.III (R) N.º 2200/114, se crea el Centro Conjunto para Operaciones de Paz de Chile. Desde su origen, este centro se concibió como una entidad conjunta e integrada<sup>6</sup>” (CECOPAC, 2021, p. 2), enriqueciendo su quehacer al considerar las diversas perspectivas de los actores involucrados en las OPAZ.

Dependiente del Ministro de Defensa Nacional a través del Estado Mayor Conjunto, el CECOPAC opera con una visión nacional, facilitando un enlace fluido con organismos vinculados a las Operaciones de Cooperación Internacional. Con el paso de los años, ha consolidado su rol en la sociedad, especialmente en el ámbito de la defensa, posicionándose como un centro docente que imparte conocimientos y doctrina sobre OPAZ. Además, es la única organización certificadora de la preparación del personal que Chile comisiona para estas misiones. La historia de las OPAZ y la participación de Chile en ellas están profundamente conectadas con la necesidad de un enfoque logístico eficiente y anticipado; este enfoque no solo es decisivo para la ejecución de estas misiones, sino que también fortalece la capacidad de las fuerzas chilenas para enfrentar diversos desafíos en los contextos de despliegue.

---

<sup>6</sup> Incluyendo a personal de las Fuerzas Armadas, Orden y Seguridad Pública, así como civiles.

## **La Función Logística y la logística de anticipación en la doctrina nacional**

La logística, según la Real Academia de la Lengua Española (RAE), se define como un conjunto de medios y métodos necesarios para llevar a cabo la organización de un servicio, especialmente de distribución; agregando que, en el contexto militar: “la logística es esencial para el movimiento y mantenimiento de las tropas en campaña”. (RAE, 2024, def. 3). Por su parte, la doctrina institucional (2021) destaca la función logística como:

*El conjunto de tareas, métodos y actividades afines orientadas a una misma finalidad, que se realizan por intermedio de las diferentes unidades de apoyo logístico para dar satisfacción de las necesidades de vida y de combate de las tropas, conformando el nivel ejecutivo de la logística en la concepción del apoyo.* (RDL- 20001, 2021, p.118).

Es decir, el desarrollo eficaz de las operaciones militares; en consecuencia, la logística anticipada se convierte así en una herramienta clave para optimizar recursos y asegurar una respuesta efectiva en OPAZ.

Asimismo, cobra relevancia lo establecido en la Política de Defensa Nacional (2020), en el marco de la Cooperación Internacional y Apoyo a la Política Exterior, donde se destaca la necesidad de: “Mantener un alto grado de interoperabilidad con otros países de interés, que permita integrar fuerzas multinacionales para participar en operaciones de paz, de ayuda humanitaria y de protección de las rutas de comercio internacional, entre otras” (PDN, 2020, p. 64).

También, el Manual de Apoyo Logístico resalta que la logística es clave para planificar los recursos necesarios que permitan a las fuerzas cumplir sus misiones de manera eficiente, tanto en operaciones de guerra como en OPAZ; por su parte, la Dirección de Logística, según el Reglamento del Estado Mayor General del Ejército, asesora al Comandante en Jefe en temas logísticos, garantizando que las capacidades militares sean adecuadas para operaciones nacionales e internacionales, incluyendo la participación en OPAZ.

De esta forma, la doctrina institucional subraya que la fuerza terrestre deberá ser sostenible, y las unidades deberán contar con los medios necesarios para satisfacer sus necesidades. Este enfoque también aplica a la logística anticipada, dado que de esta forma permite prever y gestionar los recursos de manera que se garantice la capacidad operacional en todo momento.

Por otra parte, se puede señalar que la globalización y la deslocalización han aumentado la dependencia de las economías nacionales de sus redes y de transporte internacional. Esto ha llevado a la industria a enfrentar el reto de ofrecer productos con ciclos de vida más cortos y mayor valor agregado, exigiendo una disponibilidad casi inmediata.

Ante este escenario, surge la necesidad de un modelo predictivo para implementar una logística anticipada. Según el BID (2017), el uso de herramientas como Big Data "proporcionará a las organizaciones la capacidad de planificar y ejecutar sus estrategias fundamentadas en datos predictivos" (BID, 2017, p. 24). Este concepto, surgido en la gestión de cadenas de suministro y relacionado con la inteligencia artificial, se centra en la "Mejora de la Experiencia de los Clientes", lo que conlleva la implementación de sistemas avanzados que gestionan múltiples variables para "predecir" con un margen de error mínimo las necesidades de los usuarios.

En este contexto, la logística en las OPAZ es esencial para garantizar la planificación y provisión de recursos necesarios para el éxito de las misiones; este enfoque integral cubre desde el despliegue inicial hasta la sostenibilidad de las operaciones, enfrentando desafíos como infraestructuras dañadas o entornos impredecibles. Además, la coordinación con actores clave, como gobiernos anfitriones y organizaciones internacionales, asegura la adaptabilidad y eficiencia para cumplir con los mandatos establecidos; permitiendo una respuesta efectiva, sino que también refuerza la capacidad operativa y el impacto de las fuerzas desplegadas; esta capacidad se refleja en la anticipación de las necesidades logísticas de las misiones, asegurando una respuesta más ágil y precisa en situaciones críticas.

Al respecto, cobra relevancia el Memorándum de Entendimiento (MOU) como documento clave en las OPAZ, ya que establece la cooperación entre la ONU y los países contribuyentes, definiendo aspectos esenciales como la movilización de recursos, protocolos de comunicación y responsabilidades; este acuerdo proporciona un marco claro para la colaboración internacional, asegurando que todos los participantes comprendan sus roles y obligaciones, lo que facilita una coordinación eficiente y efectiva en entornos complejos y desafiantes, fundamental para el éxito de las misiones de paz.

Derivado de lo anterior, la "logística de anticipación" se encargará de gestionar el envío de recursos antes de formalizar las solicitudes, permitiendo que las organizaciones se preparen con antelación para responder rápidamente en crisis. Este enfoque optimiza los tiempos de reacción y asegura que las operaciones se adapten de manera efectiva a los desafíos del terreno, garantizando el cumplimiento

de los mandatos. Al respecto, Gómez (2018) menciona las ventajas que ofrece el uso de la logística anticipada o predictiva en las operaciones, entre las cuales se destacan:

- a. **Gestión de Costes:** La logística anticipada ayuda a reducir costos directos e indirectos al prever la disminución de la demanda de servicios logísticos y detectar posibles retrasos en las rutas, así como identificar mercancías que requieren cuidados especiales durante el embalaje.
- b. **Planificación de Capacidades Logísticas:** Alinear las capacidades logísticas con la demanda permite hacer previsiones precisas y ajustar los recursos necesarios para evitar vacíos en la oferta.
- c. **Pronósticos de Mantenimiento:** El análisis de datos permite identificar los momentos óptimos para el mantenimiento y sustitución de equipos, garantizando la disponibilidad y operatividad de los recursos.
- d. **Envíos Anticipados:** Programar con antelación mejora la eficiencia del transporte y agiliza el proceso logístico, gracias a un modelo de gestión más dinámico (Gómez, 2018).

Cabe señalar que el concepto de “Logística Anticipada” podría definirse como la capacidad logística para prever recursos y gestionar procesos, mejorando así la eficiencia al anticipar la demanda; esta definición es crítica en OPAZ, donde una respuesta rápida puede determinar el éxito de la misión. Además, la función logística en las OPAZ debe adaptarse al contexto específico de cada misión, garantizando procedimientos eficientes tales como el abastecimiento y transporte.

En la anticipación de una OPAZ, las funciones logísticas claves incluyen transporte, abastecimiento de recursos esenciales, instalación de alojamientos y comunicación para garantizar la respuesta inmediata. El mantenimiento técnico, se desarrolla según las necesidades de la misión, ajustando los recursos de manera flexible a los desafíos del entorno operativo.

La logística anticipada resulta esencial para preparar al personal desplegado y responder adecuadamente a las necesidades de la autoridad, contribuyendo a la estabilidad de las misiones. Conocer las características geográficas del terreno permite anticipar requerimientos logísticos y facilitar el transporte, al tiempo que se identifican posibles dificultades. Así, la logística anticipada optimiza recursos y asegura que las fuerzas estén bien equipadas para enfrentar desafíos en entornos cambiantes, cumpliendo con los requerimientos establecidos.

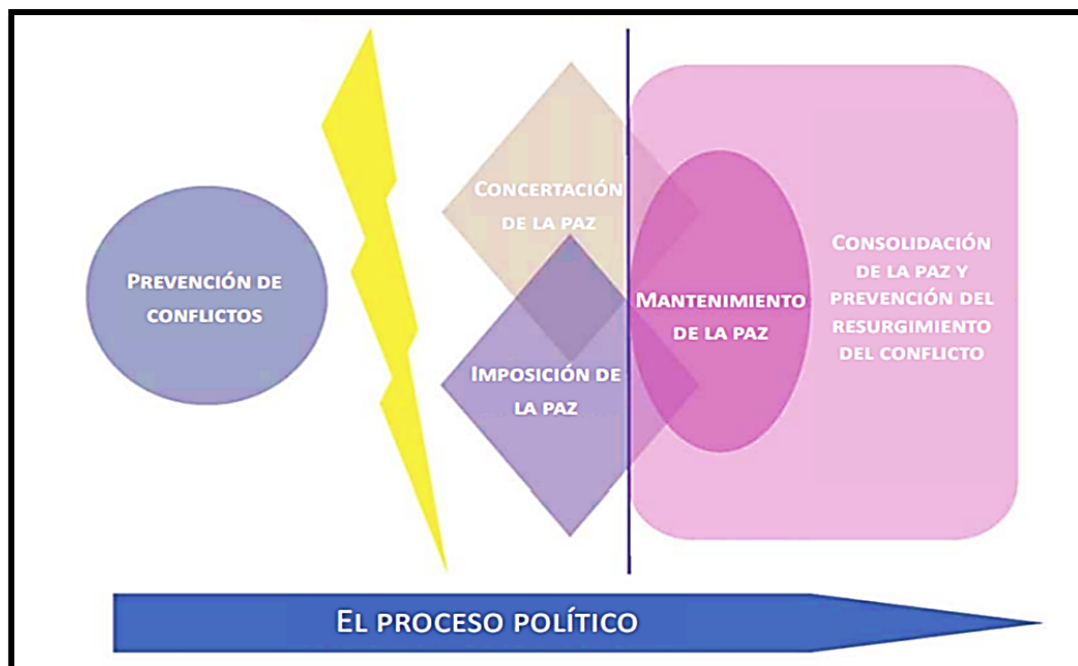
En consecuencia, la “logística anticipada” es fundamental en OPAZ, optimiza recursos y asegura que las fuerzas estén bien equipadas ante desafíos en entornos cambiantes. Para satisfacer los requerimientos, es crucial entender cómo se aplica la logística en cada contexto específico.

### La Función Logística en el marco de las OPAZ

La logística en el marco del Sistema de las Naciones Unidas se planifica y ejecuta considerando el entorno operativo y las medidas que el Consejo de Seguridad puede autorizar, siendo el mantenimiento de la paz una de estas actividades. Estas operaciones, a menudo vinculadas a la prevención y resolución de conflictos y la consolidación de la paz, respaldan ceses del fuego y acuerdos de paz, contribuyendo también a las fases iniciales de consolidación. Por lo tanto, es esencial que el personal de mantenimiento de la paz y los planificadores logísticos comprendan la interrelación entre estas actividades, ya que sus acciones pueden favorecer tanto el mantenimiento de la paz como la prevención de conflictos.

#### Figura N° 1

*El proceso político en la resolución de conflictos en el Sistema de las Naciones Unidas.*



*Nota:* Apoyo logístico a las operaciones de mantenimiento de la paz de las Naciones Unidas. Instituto para Formación en Operaciones de Paz (2018).

## **Prevención de Conflictos**

La prevención de conflictos en el marco del Sistema de Naciones Unidas implica la implementación de medidas diplomáticas y/o herramientas diversas para evitar que las tensiones entre estados o dentro de ellos se conviertan en conflictos violentos. Generalmente, se trata de una medida pacífica adaptada a la causa específica de la disputa o tensión; al respecto, la prevención de conflictos puede incluir el diálogo, mediación, investigación de las causas del desacuerdo o medidas para fomentar la confianza, un enfoque común en la prevención de conflictos es la utilización de los "buenos oficios" del Secretario General de la ONU como mediador, para facilitar el diálogo entre las partes, con el fin de reducir tensiones, mediar en desacuerdos o ayudar a resolver conflictos.

También se puede solicitar a organizaciones regionales que intervengan para asistir en la prevención de conflictos, en esta línea de ideas, el apoyo logístico a una misión dedicada a la prevención de conflictos puede ser tan simple como proporcionar una Dieta de Misión (MSA, por su sigla en inglés) para cubrir los gastos de supervivencia de los integrantes del personal destacados a una misión especial; adicionalmente, puede ser necesario facilitar transporte terrestre utilizando vehículos de la ONU o mediante arrendamiento entre otros.

### *Concertación de la Paz*

La concertación de la paz en el Sistema de Naciones Unidas implica medidas destinadas a abordar conflictos en curso y suele requerir intervención diplomática para lograr que las partes acepten negociar un acuerdo.

Esto puede incluir acciones directas por parte de las Naciones Unidas para facilitar la negociación de un acuerdo de paz, además de ayudar a los negociadores de paz regional o internacional, ofreciendo una ubicación neutral para las negociaciones o presidiendo las sesiones; al respecto, el Consejo de Seguridad puede solicitar al Secretario General o a otros actores relevantes de la concertación de la paz que intervengan en este proceso.

Asimismo, gobiernos, grupos de estados o personalidades destacadas pueden llevar a cabo esfuerzos de concertación de la paz. “Uno de los primeros ejemplos de iniciativa de concertación de la paz de la ONU fue la designación del diplomático sueco Conde Folke Bernadotte como mediador de la ONU en Palestina en 1948, a fin de utilizar “sus buenos oficios para promover una solución pacífica para el futuro de Palestina” (Little, 2018, p. 22).

Aunque la concertación de la paz no se menciona explícitamente en la Carta de las Naciones Unidas, su fundamento jurídico puede variar desde simples hasta complejos, dependiendo de las circunstancias del área de misión. Cuando los responsables de la planificación logística del Departamento de Apoyo de las Operaciones (DAO) comienzan a elaborar el plan logístico, factores clave como el alcance del conflicto y el mandato autorizado por el Consejo de Seguridad tuvieron que ser cuidadosamente considerados, ya que una operación de concertación de la paz difiere significativamente de un mandato orientado a la prevención de conflictos.

### *Imposición de la Paz*

Como su nombre indica, la imposición de la paz es un enfoque más contundente que las operaciones humanitarias o de protección. A diferencia del mantenimiento de la paz, no hay un proceso de paz en curso ni consentimiento de las partes en conflicto; al respecto, el capítulo VII de la Carta de la ONU establece los fundamentos jurídicos para este tipo de operaciones; en general, la ONU no interviene directamente en la imposición de la paz; en cambio, puede recurrir a organizaciones regionales para que adopten medidas en virtud del capítulo VIII de la Carta; de esta forma, la ONU podría llegar a emprender “acciones contundentes de mantenimiento de la paz”, que es cuando se despliega una operación de mantenimiento de la paz de la ONU con el consentimiento de las principales partes en conflicto (Little, 2018, p. 23); motivo por el cual, la imposición de la paz planteará desafíos logísticos a la ONU que requieren una planificación cuidadosa y recursos significativos para que involucre la imposición de la paz, ya que la seguridad de los pacificadores puede depender de ello; implementación; siendo esencial contar con todo el apoyo logístico necesario para cumplir con cualquier mandato de esta forma, la protección de las fuerzas, será por tanto, un factor trascendental en la planificación logística.

### *Mantenimiento de la Paz*

El mantenimiento de la paz es una técnica destinada a preservar la estabilidad tras un conflicto y a facilitar la implementación de los acuerdos entre las partes involucradas. Las operaciones de la ONU se llevan a cabo cuando las partes han acordado un cese del fuego, requiriendo su consentimiento para establecer las bases de una paz sostenible.

Con el tiempo, el mantenimiento de la paz ha evolucionado de un enfoque militar tradicional a uno más complejo, que integra actores militares, civiles y policiales. Para el éxito de estas operaciones, es vital que la ONU implemente un modelo logístico flexible e integrado. Aquí, la logística anticipada cobra especial relevancia,

ya que permite una planificación proactiva que adapta los recursos a las circunstancias cambiantes, mejorando así la eficiencia operativa.

La estabilización de un conflicto es solo el primer paso hacia una paz duradera. Es fundamental implementar medidas que mitiguen el riesgo de recaídas en la violencia, consolidando la paz a través de estrategias que fortalezcan la capacidad nacional para gestionar conflictos y fomenten el desarrollo sostenible. Las operaciones multidimensionales de mantenimiento de la paz incluyen el apoyo a la reconstrucción del estado y abordan causas estructurales del conflicto, como la reforma del sector de la seguridad (SSR), lo cual es clave para mejorar la efectividad del Estado.

Desde el punto de vista logístico, el apoyo a la consolidación de la paz se apoya en iniciativas previas, haciendo que la logística anticipada sea crucial para asegurar que los recursos se ajusten rápidamente a las necesidades emergentes, lo que a su vez contribuye al éxito de la consolidación de la paz.

### **Conceptos de logística de la ONU**

Según el sistema logístico de la ONU, las unidades de los Estados Miembros en misión deben tener autonomía inicial de entre 30 y 90 días, e incluso hasta 180 días en algunos casos. Este período es trascendental para que la ONU organice el cuartel general de la misión y establezca la estructura logística necesaria, así como para adquirir propiedades y finalizar acuerdos locales; durante este tiempo, la ONU proporcionará suministros esenciales como agua, combustible y raciones, además de apoyo en alojamiento y servicios básicos; al respecto, la implementación de la logística anticipada es esencial, ya que permite que los expertos en logística informen a los comandantes sobre la necesidad de planes de auto sustentación para el contingente. A pesar de la presencia de equipos de la ONU, la preparación anticipada es clave para la eficacia operativa.

De esta forma, el apoyo logístico deberá adaptarse a cada misión específica, dado que las dimensiones de las operaciones de la ONU varían desde pequeños grupos hasta grandes operaciones combinadas; donde la logística anticipada ajusta este apoyo a factores críticos<sup>7</sup>.

---

<sup>7</sup> Tareas, espacio, tiempo, recursos humanos, clima e infraestructura.

## Herramientas de planificación logística

Los responsables de la planificación logística realizarán estimaciones iniciales considerando las cuatro D<sup>8</sup>. Durante la fase de pre-despliegue, es fundamental realizar una evaluación exhaustiva del entorno logístico del destino de la misión, que determinará no solo el desgaste de equipos, sino también las exigencias fisiológicas que enfrentarán los pacificadores. Se deben evaluar riesgos, requerimientos de suministros y la infraestructura de transporte, lo que permite una logística anticipada más efectiva.

- **Distancia:** La consideración de las distancias estratégicas dentro del teatro de operaciones es esencial, ya que afecta la composición de los recursos logísticos asignados. Conocer las rutas de abastecimiento y los índices de tráfico es fundamental para una planificación anticipada.
- **Demanda:** La demanda logística se define según el tipo de misión y el área de operaciones, evaluando el consumo de material y las actividades previstas. Esto asegura que los planes de logística anticipada se ajusten a las necesidades reales.
- **Duración:** La duración indefinida de la misión debe considerarse desde el inicio, planteando una autonomía logística mínima de 90 días. La planificación anticipada incluye preparativos para el eventual retiro.
- **Destino:** Las misiones de mantenimiento de la paz suelen desarrollarse en entornos austeros con escasa infraestructura. Por ello, durante la fase de pre-despliegue, es necesario llevar a cabo una evaluación logística detallada del destino para garantizar una logística anticipada eficaz.

Por otra parte, el entorno influirá en el desgaste de los equipos, las exigencias fisiológicas del personal y los niveles de protección de la fuerza, lo que exige una planificación de logística anticipada para mitigar estos impactos.

La planificación logística inicial es un proceso que requiere abordar diversos factores mientras se mantiene la flexibilidad necesaria para adaptarse a los cambios en los requerimientos, siendo fundamental que quienes están a cargo de esta planificación tengan claridad sobre los objetivos operativos, las capacidades de suministro disponibles y las fuentes de abastecimiento en la zona de misión; este enfoque proactivo no solo contribuye a optimizar la eficiencia de la misión, sino que también garantiza que se aprovechen al máximo las capacidades de suministro de las fuerzas involucradas y de los recursos del país anfitrión.

---

<sup>8</sup> Distancia, demanda, duración y destino.

Para lograrlo, el objetivo primordial durante la fase de planificación logística previa es definir con precisión el requerimiento de apoyo operativo; para este fin, se utilizan herramientas de planificación, como el cálculo estimativo de logística y el análisis de limitaciones, que permiten identificar los requerimientos logísticos específicos de la misión; en este contexto, la anticipación en la obtención de valores estimativos se vuelve crucial, ya que ayuda a determinar si es más eficiente utilizar recursos militares o depender del país anfitrión. Este proceso de evaluación asegura que se aborden de manera efectiva las necesidades logísticas.

Por otro lado, las Naciones Unidas proporcionan apoyo a través de su infraestructura global, que incluye la Secretaría en Nueva York y las sedes de la ONU en diversas ciudades. Además, pueden recibir contribuciones de países miembros, quienes a menudo ofrecen apoyo logístico para cubrir necesidades específicas, incluyendo personal y materiales. En este sentido, es esencial coordinar estas contribuciones con las de la ONU para integrar adecuadamente todos los elementos en la planificación logística anticipada.

El tiempo necesario para desplegar una misión puede variar considerablemente según la disposición de los Estados Miembros para aportar recursos. La fase de "puesta en marcha de la misión" implica establecer procesos y servicios que permitan alcanzar una capacidad operativa mínima. Durante este despliegue inicial, un equipo de avanzada cuya misión es facilitar la llegada de más personal y contingentes, asegura que la misión pueda comenzar de manera eficiente.

Además, la reserva estratégica otorga a la ONU la capacidad de realizar misiones de mantenimiento de la paz de manera oportuna. Rod Little (2018) señala que: "Un componente clave para el éxito de la puesta en marcha de una misión es el despliegue rápido, lo cual exige contar con los equipos de reserva a ser enviados al terreno" (p.16), lo cual requiere contar con equipos de reserva que puedan ser proyectados al terreno según sea necesario. Esta reserva incluye acuerdos de personal militar y civil, así como materiales gestionados en el Centro de Apoyo Mundial, lo que refuerza la efectividad de la misión.

Finalmente, el reconocimiento logístico juega un papel fundamental en la planificación anticipada. Little (2018) afirma que "el tiempo dedicado al reconocimiento nunca es tiempo perdido" (p. 121). Por esta razón, es importante que el personal encargado de la planificación realice visitas al área de misión para evaluar la capacidad de apoyo del país anfitrión y la infraestructura disponible. Así, la logística anticipada se revela esencial para garantizar un despliegue eficiente y sin obstáculos, permitiendo que todos los aspectos logísticos que puedan limitar el

plan operativo sean comunicados adecuadamente en un informe detallado que beneficie a todas las partes interesadas.

## **Conclusiones**

El análisis presentado destaca la logística anticipada como un elemento fundamental para el éxito de las OPAZ de la ONU; en un entorno cada vez más complejo, será fundamental contar con un sistema logístico que no solo responda a las necesidades inmediatas, sino que también anticipe futuras demandas, permitiendo una actuación rápida y efectiva que minimice riesgos para el personal militar y las poblaciones civiles afectadas.

Al respecto, la historia ha demostrado que la efectividad logística es vital para el logro de los objetivos de las misiones de paz; casos como la crisis de Darfur evidencian que una estructura logística bien diseñada facilita el cumplimiento de las metas estratégicas y establece un entorno seguro para la ejecución de operaciones; así, la logística anticipada refuerza la capacidad de protección de civiles y la credibilidad de las operaciones de la ONU.

Por otra parte, el contexto geopolítico actual exige una constante adaptación de las estrategias logísticas, priorizando la distribución de recursos según las necesidades específicas de cada grupo involucrado; dicha planificación proactiva será crucial no solo para el éxito de las misiones, sino también para construir una paz sostenible, asegurando que los recursos estén disponibles en el momento y lugar adecuados. Es esencial que la logística anticipada se integre como un elemento estratégico en la planificación de OPAZ; su adopción garantizará un despliegue eficiente de las fuerzas y contribuirá a establecer un entorno de seguridad en los países anfitriones. Reconocer su importancia es vital para maximizar la efectividad de las futuras misiones.

Desarrollar una logística anticipada es más que un componente técnico; es una estrategia que potencia la efectividad operativa. La implementación de modelos predictivos, impulsados por avances tecnológicos y la inteligencia artificial, permitirán anticipar demandas y mejorar la calidad del servicio logístico, siendo indispensable en un contexto de globalización. Al respecto, se sugiere que la doctrina institucional adapte los procedimientos referentes al concepto de logística anticipada a las características de las OPAZ; dado que esta estrategia será esencial para garantizar la estabilidad en entornos operativos complejos.

Así también será fundamental integrar la logística anticipada en los planes operativos, asegurando que todos los niveles de mando comprendan su relevancia y estén capacitados para implementarla eficazmente.

En consecuencia, una logística anticipada y flexible será indispensable para el éxito de las operaciones de la ONU, garantizando el cumplimiento de los objetivos de paz y seguridad. Invertir en capacidades logísticas anticipadas es invertir en estabilidad y paz, preparando a las fuerzas de mantenimiento no solo para intervenir, sino también para fomentar un entorno pacífico y sostenible en regiones afectadas.

## Referencias

- Banco Interamericano de Desarrollo (BID) (2017). “*Estrategia Logística Nacional de Panamá a 2030*”. Recuperado de: <https://www.presidencia.gob.pa/pdfs/Estrategia%20Logistica%20Nacional%202030%20-%20Documento%20Final2017.pdf>
- Cruz S. (2019). El uso de la fuerza en operaciones de paz: tres casos en África. JE 4 – Economía Política, Política Internacional y Relaciones Internacionales. Fundación de Pesquisa del Estado de Sao Paulo (FAPESP). Recuperado de: <https://alacip.org/cong19/72-aguilar-19.pdf>
- Ejército de Chile (2011). Manual Función Logística (MDO- 90906). Santiago, Chile: DIVDOC.
- Ejército de Chile. (2011). Diccionario Militar (MDO-90906). Santiago, Chile: DIVDOC.
- Ejército de Chile (2021). Reglamento Logística (RDL- 20001). Santiago, Chile: DIVDOC.
- Ejército de Chile (2021). Reglamento Apoyo Administrativo (RDP- 20001). Santiago, Chile: DIVDOC.
- Estado de Sao Paulo (FAPESP). Recuperado de: <https://alacip.org/cong19/72-aguilar-19.pdf>

- Gómez Ch. (2018). “Ventajas del uso de la logística predictiva”; Servicios de transporte, Sertrans España. Recuperado de: <https://www.sertrans.es/trasporte-terrestre/la-dualidad-de-la-logistica-predictiva-y-el-transporte-por-carretera>
- Gobierno de Chile (2020). Política de Defensa Nacional. Ministerio de Defensa. Santiago. Recuperado de: <https://www.defensa.cl/wp-content/uploads/2023/06/POL%C3%8DTICA-DE-DEFENSA-NACIONAL-DE-CHILE-2020.pdf>
- Instituto Español de Estudios Estratégicos. (2015). Estudio Sobre La Posibilidad De que un Operador de Apoyo Logístico Conjunto, Apoye en todas las Funciones Logísticas. Obtenido de Instituto Español de Estudios Estratégicos: [http://www.ieee.es/Galerias/fichero/docs\\_trabajo/2015/DIEEET08-2015\\_OperadorApoyoLog\\_FuncionesLogisticas\\_MOPS.pdf](http://www.ieee.es/Galerias/fichero/docs_trabajo/2015/DIEEET08-2015_OperadorApoyoLog_FuncionesLogisticas_MOPS.pdf)
- Little R. (2018). Apoyo logístico a las operaciones de mantenimiento de la paz de las Naciones Unidas: Introducción. Instituto para Formación en Operaciones de Paz. Recuperado de: [https://www.peaceopstraining.org/fr/courses/log1-es-2021/?reviews\\_page=4](https://www.peaceopstraining.org/fr/courses/log1-es-2021/?reviews_page=4)
- Ministerio de Defensa (2014). Doctrina logística para el empleo conjunto de la fuerza (DNC 4-0). Doctrina Nacional Conjunta. República de Chile.
- Organización de las Naciones Unidas (ONU) (2024). Años preparatorios: Historia de la Carta de la ONU. Recuperado de: <https://www.un.org/es/about-us/history-of-the-un/preparatory-years>
- Soria M. (1998). Logística Multinacional. Boletín de información. Ministerio de Defensa: Centro Superior de Estudios de la Defensa Nacional. España. Recuperado de: <https://dialnet.unirioja.es/descarga/articulo/4643297.pdf>
- Valenzuela J. (2017). Aproximación conceptual a la función sostenimiento de las fuerzas en las operaciones militares. Revista Ensayos Militares Vol. 3 N°2. Año 2017. Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile. Recuperado de: <https://revistaensayosmilitares.cl/index.php/acague/article/view/69/70>
- Vargas C. (2024). Una mirada al sistema de apoyo logístico del Ejército de Tierra Español, algunas ideas. Centro de Estudios e Investigaciones Militares (CESIM). Memorial del Ejército de Chile, N° 514, p. 103. Ejército de Chile.



# MOVILIDAD ESTRATÉGICA: EL ROL DEL FERROCARRIL EN LA LOGÍSTICA MILITAR

## *Strategic Mobility: The Role of the Railway in Military Logistics*

Mayor Sergio Villaseca Zanzi<sup>1</sup>

**Resumen:** El ferrocarril ha jugado un papel fundamental en la movilidad estratégica militar al facilitar el transporte eficiente y rápido de tropas y suministros a grandes distancias. Desde su aparición en el siglo XIX, permitió la movilización masiva en conflictos importantes como la Primera y Segunda Guerra Mundial, siendo un medio clave para el despliegue y abastecimiento. Actualmente, su importancia se revitaliza en el conflicto en Ucrania, donde tanto Rusia como Ucrania dependen de las redes ferroviarias para sostener sus operaciones logísticas. La modernización de esta infraestructura es esencial para asegurar una respuesta rápida en escenarios de crisis, destacando el valor estratégico del ferrocarril en la defensa nacional y en alianzas internacionales como la OTAN.

**Palabras clave:** Movilidad Estratégica, Ferrocarril, Logística

**Abstract:** Railways have long played a fundamental role in strategic military mobility by facilitating the efficient and rapid transport of troops and supplies over long distances. Since their appearance in the 19th century, they have enabled mass mobilization in major conflicts such as the First and Second World Wars, being a key means of deployment and supply. Today, their importance is revitalized in the conflict in Ukraine, where both Russia and Ukraine rely on railway networks to sustain their logistical operations. The modernization of this infrastructure is essential to ensure a rapid response in crisis scenarios, highlighting the strategic value of railways in national defense and in international alliances such as NATO.

**Keywords:** Strategic Mobility, Railway, Logistics

---

<sup>1</sup> Oficial de Estado Mayor del arma de Caballería Blindada. Licenciado en Ciencias Militares de la Academia de Guerra del Ejército de Chile. Actualmente se desempeña como comandante de la Compañía Logística y Administrativa N°4 "Concepción" del Regimiento N°6 "Chacabuco". Correo electrónico: [sergio.villaseca@ejercito.cl](mailto:sergio.villaseca@ejercito.cl)

## Introducción

Con la llegada del ferrocarril en el siglo XIX, rápidamente revolucionó al mundo como medio de transporte terrestre por su ventaja cualitativa como medio de transporte masivo. La capacidad que entregaba la locomotora a vapor permitió que la carga de pertrechos y transporte de tropas fuera a gran escala durante la guerra franco-prusiana en 1870, revolucionando la logística militar. Sin embargo, su potencial empleo con fines bélicos lo alcanzó durante la I Guerra Mundial, convirtiéndose en el principal medio de transporte ante la electrificación e irrupción de motores a combustión interna para este medio de carga (Thompson & Angerstein, 2000). Su rol se hizo fundamental al permitir el transporte rápido de tropas, armas y suministros a grandes distancias, transformándose en una herramienta clave para el sostenimiento de la guerra.

Durante la Segunda Guerra Mundial (IIGM), su uso también posibilitó el movimiento estratégico de los ejércitos, permitiendo céleres campañas, permitiendo alcanzar objetivos estratégicos con rapidez. Terminada la guerra, en la segunda mitad del siglo XX, la construcción masiva de autopistas redujo la relevancia del transporte ferroviario, mientras que el transporte aéreo comenzó a dominar los viajes a larga distancia. El tren fue desplazado ante el empleo de vehículos terrestres como camiones y transportadores sobre ruedas, capaces de ir de un punto a otro de un país o de una región, evitando la necesidad de trasbordos, haciendo menos rentable el transporte sobre vías a distancias medias.

Sin embargo, las características únicas que proporciona el ferrocarril, no solo han facilitado el movimiento de grandes volúmenes de carga a largas distancias, sino que también proporciona una red de movilidad flexible y resiliente, capaz de apoyar operaciones tanto a nivel nacional como internacional. En un entorno globalizado donde los desafíos de seguridad son cada vez más complejos, el rol del ferrocarril en la logística militar se convierte en un factor esencial para garantizar la capacidad de respuesta rápida y efectiva de las fuerzas armadas, en especial para el abastecimiento y transporte de medios de un ejército.

Este artículo argumenta que, a pesar de los avances en tecnología y la diversificación de los métodos de transporte militar, el ferrocarril sigue siendo un componente indispensable en la logística militar. Su eficiente capacidad como medio de transporte de cargas pesadas y su flexibilidad en la integración en redes logísticas modernas, lo convierte en un factor decisivo en la planificación y ejecución de operaciones militares a gran escala.

Este artículo explora cómo el ferrocarril logró su posición como medio de transporte en la guerra y como contribuyó a la movilidad estratégica, analizando sus capacidades, restricciones y beneficios. Además, tiene la intención de entregar un panorama actualizado en las operaciones de movimiento y transporte, para reimpulsar y adecuar la infraestructura ferroviaria para el uso de las fuerzas armadas.

## **La movilidad estratégica**

Conceptualizando la movilidad estratégica, este término se define en nuestra doctrina como la capacidad de trasladar unidades a un teatro de operaciones. Esta movilidad depende de los recursos y capacidades de las unidades y de los sistemas de transporte disponibles a nivel nacional. Es fundamental tener la habilidad de desplazar fuerzas a grandes distancias en plazos reducidos, ocupando posiciones estratégicas y facilitando operaciones militares cuando sea necesario (Ejército de Chile, 2011). Para la OTAN, este concepto la define como la capacidad para desplegar rápida y eficazmente las distintas fuerzas y su apoyo logístico entre teatros (interteatro), entre regiones (interregional), o fuera del área de responsabilidad (Hernández Tortajada, 1999).

En cambio, la doctrina nacional conjunta no ofrece una definición precisa, pero está asociada a la logística del transporte, destacándola como esencial para la configuración del Teatro de Operaciones Conjunto (TOC), permitiendo el sostenimiento de la fuerza y satisfaciendo las necesidades logísticas. La reglamentación enfatiza la importancia del transporte como factor crítico para asegurar la movilidad en el TOC, fundamental para el éxito de las operaciones (Ministerio de Defensa Nacional, 2014).

Para clarificar, la función de transporte se refiere a los métodos usados para trasladar tropas y suministros desde un origen hasta su destino. Se centra en la coordinación logística, abarcando planificación, ejecución y gestión de diversos modos de transporte, ya sea terrestre, aéreo o marítimo, y su combinación (multimodal). El objetivo es garantizar que las fuerzas tengan acceso a recursos en el momento y lugar adecuados, considerando la planificación de rutas, selección del medio, manejo de cargas y coordinación (Ministerio de Defensa Nacional, 2014).

Por otro lado, la movilidad estratégica abarca la capacidad general de las fuerzas para desplazarse a través de amplios espacios geográficos y adaptarse a necesidades operacionales. Para la doctrina norteamericana, preservar esta movilidad permite a los comandantes controlar el tempo y dinámica de las operaciones, posicionando fuerzas y recursos para cumplir objetivos estratégicos y

tácticos. Así, asegurar la movilidad estratégica maximiza la flexibilidad y efectividad en el campo de batalla (Joint Chiefs of Staff, 2020).

Para lograr la movilidad estratégica, se requieren medios de transporte adecuados, que la doctrina conjunta nacional operacionaliza en tres niveles: estratégico, operativo y táctico. Los medios de transporte necesarios para la movilidad estratégica están en el primer nivel. El transporte estratégico se define como “la capacidad de trasladar fuerzas, abastecimientos, material y equipo, rápidamente a largas distancias, utilizando medios terrestres, aéreos o navales” (Ministerio de Defensa Nacional, 2014).

Los medios aéreos y navales son, en esencia, estratégicos por su capacidad de proyectar fuerzas a largas distancias. Sin embargo, el transporte terrestre no determina uno específico, sino “adecuado”<sup>2</sup>. De acuerdo con esta definición, el ferrocarril se presenta como el medio más eficiente para el transporte estratégico terrestre. Esto distingue la importancia histórica del ferrocarril en operaciones militares y su relevancia actual.

### **Breve análisis histórico del ferrocarril como medio de transporte estratégico hasta la IIGM**

El General Helmuth von Moltke<sup>3</sup> fue pionero en reconocer la importancia de los ferrocarriles para el despliegue, movimiento y suministro de grandes ejércitos. Antes de su visión, el movimiento de tropas estaba limitado por la escasez y falta de fiabilidad de las carreteras, restringiendo las acciones a pequeños campos de batalla. Moltke entendió que los ferrocarriles permitían una movilización más rápida y eficiente, ampliando los frentes de combate a cientos de kilómetros. Esto transformó las maniobras militares de simples flanqueos a movimientos envolventes con múltiples divisiones. Gracias a los ferrocarriles, las tropas podían mantenerse en el campo de batalla en cualquier clima y durante todo el año (Barclay, 2024).

---

<sup>2</sup> Probablemente la palabra seleccionada se explicaría producto que Chile, al contar con una red ferroviaria limitada, no podría satisfacer las necesidades que requería el Ejército o las Fuerzas Armadas para realizar movimientos hacia o desde un TOC.

<sup>3</sup> Helmuth Karl Bernhard von Moltke (1800-1891), también conocido como Moltke el Viejo, fue un mariscal de campo alemán cuyo genio militar ayudó a convertir a Prusia en el Estado hegemónico en Alemania. Jefe del Estado Mayor General prusiano durante treinta años, es considerado el creador de una nueva forma de dirigir los ejércitos sobre el terreno, así como el arquitecto militar de la unificación alemana.

Similarmenle, el general William Tecumseh Sherman<sup>4</sup> usó la red ferroviaria durante la Guerra Civil norteamericana, donde los ferrocarriles desempeñaron un papel crucial por su eficacia, confiabilidad y rapidez, superando a otros medios de transporte. El tren podía transportar casi cincuenta veces más carga y no se veía afectado por las condiciones climáticas, reduciendo el costo del transporte en un 95%. El Ejército de la Unión aprovechó estratégicamente la red ferroviaria, permitiendo combatir en regiones remotas y transportando suministros directamente al frente. Los ferrocarriles se convirtieron en objetivos estratégicos, y su red en el Sur, menos desarrollada, se deterioró durante la guerra, limitando la capacidad del ejército confederado. Durante este conflicto, aparecieron los primeros modelos de ferrocarriles blindados (Smithsonian Institution, 2015).

Al igual que Moltke, el general Sherman durante la Guerra Civil norteamericana utilizó la red ferroviaria en beneficio de la Unión. La importancia de los ferrocarriles en tierra estadounidense ya había desempeñado un papel relevante debido a su eficacia, fiabilidad y rapidez, superando a otros medios de transporte como los barcos de vapor, ya que como se mencionó anteriormente, este podía transportar más carga y su trayecto no se veía afectado por las condiciones climáticas, a diferencia de los barcos de vapor, por ejemplo.

El Ejército de la Unión aprovechó estratégicamente la red ferroviaria, contribuyendo de manera significativa a su victoria. A diferencia de guerras anteriores, en las que las batallas se libraban cerca de áreas pobladas para aprovechar los recursos locales, los ferrocarriles permitieron librar combates en regiones remotas, dejando de depender de los recursos inmediatos de la tierra ocupada. Los ferrocarriles se convirtieron en objetivos estratégicos, destacando en su uso y destrucción para debilitar a la Confederación.

Ya a principios del siglo XX, los ferrocarriles eran el principal medio de transporte terrestre. Los vehículos a motor no ofrecían una competencia significativa, salvo para el tráfico local, y la aviación estaba en sus primeras etapas de desarrollo. Debido a esta dependencia del ferrocarril, las naciones europeas construyeron sus planes de movilización y sostenimiento de sus ejércitos en torno a la infraestructura ferroviaria. Cada país había desarrollado sistemas complejos para concentrar tropas y equipos en puntos estratégicos, lo que permitía un rápido despliegue de fuerzas hacia sus fronteras.

---

<sup>4</sup> William Tecumseh Sherman (1820-1891), fue un General del Ejército de la Unión durante la Guerra Civil norteamericana. Se destacó por su victoria en la Batalla de Shiloh, la captura de Atlanta y su Marcha hacia el Mar.

En 1914, durante la Primera Guerra Mundial, las naciones europeas tras años de planificación convirtieron al ferrocarril en el eje de la movilización de tropas, demostrando ser esenciales para la campaña. Facilitaron el transporte de soldados al frente y su retorno, así como el traslado de armas y equipos desde las fábricas hasta los puntos de distribución (Derrick, 2011). La utilización de ferrocarriles blindados se expandió considerablemente durante la Primera Guerra Mundial. Los ejércitos de las potencias en guerra comenzaron a emplear trenes especiales equipados con cañones y blindaje para proteger a las tropas y surtir de suministros a las líneas del frente. Estos trenes no solo servían para el transporte, sino también como plataformas de artillería móvil, capaces de lanzar ataques en zonas donde las fuerzas eran necesarias (G.G. Lepage, 2017).

Esta planificación alcanzó su mayor nivel de sofisticación en Alemania y Francia. Por ejemplo, el famoso "Plan Schlieffen" de Alemania, dependía de la rápida concentración de tropas a lo largo de las fronteras oriental y occidental mediante el uso de trenes. El plan se basaba en la suposición de que el ejército ruso tardaría en movilizarse, lo que permitiría a Alemania avanzar rápidamente a través de Bélgica y Luxemburgo, invadir el norte de Francia, y rodear París por el norte y el oeste. Una vez que Francia se rindiera, el ferrocarril permitiría a las fuerzas alemanas cambiar rápidamente su frente contra Rusia (Imperial War Museums, 2024).

Años más tarde durante la IIGM, el uso del tren siguió teniendo una preponderancia crucial para las naciones en guerra. En el caso de Inglaterra, el ferrocarril cumplió tareas vitales para mantener el esfuerzo bélico, al transportar bastimentos para las tropas y por otro lado para abastecer de alimentos a los civiles, obligando a recortar el funcionamiento en el transporte de pasajeros. Conjuntamente a su uso como transporte de carga, este también posibilitó las operaciones de evacuación, siendo un ejemplo de ellas la operación "Pied Piper"<sup>5</sup>, acción de gran envergadura para evacuar principalmente a niños de los grandes centros urbanos. Además de la evacuación de civiles, el ferrocarril también cumplió un papel fundamental en el transporte de 338.000 hombres durante la evacuación de Dunkerque en mayo y junio de 1940 siendo un hito en la historia ferroviaria inglesa (Network Rail, 2021).

El tren no solo beneficiaría a los británicos, el éxito de la Blitzkrieg entre 1939 y 1941 de Alemania, se sustentó en el uso estratégico del ferrocarril como medio esencial de transporte. A pesar de la ambición de Hitler de contar con un ejército totalmente

---

<sup>5</sup> Pied Piper, la operación de evacuación considerada la mayor migración en la historia británica, se sostuvo ante el temor a que los bombardeos alemanes causaran muertes a civiles, lo que impulsó al gobierno a evacuar a niños, madres con bebés y enfermos de las ciudades y pueblos británicos. La evacuación se llevó a cabo en varias oleadas y en el transcurso de tres días, 1,5 millones de evacuados se enviaron a localidades rurales consideradas seguras.

motorizado, la industria alemana no pudo satisfacer con tal demanda, lo que solo resultó en la completación de 16 divisiones motorizadas en 1940, de un total de 103. Lo anterior convirtió al ferrocarril en el medio crucial para los desplazamientos a largas distancias de tropas, suministros y artillería. La capacidad de concentrar un gran número de tanques, infantería y apoyo logístico a través de los ferrocarriles permitió a Alemania ejecutar sus campañas militares de manera efectiva y rápida. Así, el ferrocarril fue fundamental para la movilización y el abastecimiento durante las exitosas operaciones de la guerra relámpago (G.G. Lepage, 2017).

Sin embargo, durante la invasión a territorio soviético a través de la Operación Barbarroja en 1941, se expuso de manera brutal las deficiencias en la logística alemana. La operación se vio gravemente afectada por restricciones en el suministro, lo que resultó en su fracaso y alteró el curso de la guerra. Además del invierno ruso que impidió el avance de las unidades acorazadas, en el aspecto logístico fue un factor crítico la dependencia de la escasa red ferroviaria rusa que limitó la velocidad de avance de las tropas alemanas. El progreso de las tropas alemanas se vio restringido por la necesidad de arreglar, convertir o construir nuevas líneas ferroviarias para adaptarse a los cambios en el ancho de vía<sup>6</sup>. Esta situación generó una especie de cuellos de botella, que ralentizaron considerablemente las operaciones. Además, Alemania enfrentaba un problema permanente de escasez de combustible, tanto de gasolina como de carbón. Desde el inicio, las posibilidades de éxito de la ofensiva eran escasas, producto de líneas de suministro sobre extendidas, más allá de sus límites naturales, llegando a un punto del colapso, lo que contribuyó de manera decisiva al fracaso de la invasión (G.G. Lepage, 2017).

Además, los ferrocarriles también se utilizaron en la deportación de millones de judíos y otros perseguidos a campos de exterminio, siendo fundamentales en el Holocausto. Al final de la guerra, los ataques aliados se dirigieron a destruir infraestructura ferroviaria crucial, obstaculizando la capacidad de Alemania para mantener sus líneas de suministro y afectando su esfuerzo bélico.

## **Post IIGM**

Si bien, el sistema ferroviario global agonizó durante la guerra fría producto de la diversificación del transporte mundial, este fenómeno afectó inclusive al sistema ferroviario de EE.UU., siendo el más extenso del mundo. El caso estadounidense

---

<sup>6</sup> El término "ancho de vía" o conocido en Chile como "trocha", se refiere a la distancia nominal entre las caras internas de los rieles, expresada en milímetros. Específicamente, se trata de la medida entre las dos caras activas de las cabezas de los rieles. El ancho de vía internacional o estándar es de 1.435 mm.

afectó significativamente la capacidad operativa en el uso militar del ferrocarril. La primera de ellas fue la degradación continua de la infraestructura ferroviaria producto del deterioro de organizaciones, infraestructura y del capital de financiamiento. Aunque los ferrocarriles se recuperaron de una crisis a finales de los años sesenta y principios de los setenta, su capacidad para el transporte militar continuó en declive, en gran parte debido a la competencia de otros modos de transporte, como camiones y aerolíneas, que desviaron tráfico y aumentaron la presión financiera.

La falta de inversiones y la falta de supervisión gubernamental limitaron la capacidad de los ferrocarriles para adaptarse, en una época en que la contenedorización<sup>7</sup> cambió la forma de transportar mercaderías, complicando aún más la situación al dificultar el transporte de material militar. Con el deterioro de la infraestructura, el desempeño durante las operaciones militares se vio gravemente afectado. Para 2006, las secuelas de este retroceso fue la falta de personal capacitado, dejando a las fuerzas armadas sin la habilidad necesaria para operar en líneas férreas, caso que también afectó unas décadas antes al Ejército de Chile.

Una de las recomendaciones para revertir esta degradación en las capacidades militares, es presentar el movimiento ferroviario como un tema estratégico, además de coordinar con las principales empresas ferroviarias en la prestación de servicios, lo que podría reducir los riesgos militares y asegurar el soporte logístico necesario para el futuro (Evenson, 2006).

## **El Sistema Ferroviario en Chile**

La historia ferroviaria de nuestro país comienza a mediados del siglo XIX, con la puesta en marcha en 1851 del tren Caldera-Copiapó a través de capitales privados. Este hito marcó el inicio de una etapa de crecimiento para el ferrocarril en Chile, porque a partir de ese momento las inversiones tanto privadas como estatales se incrementaron rápidamente. Los capitales del norte necesitaban el ferrocarril para transportar la producción minera y el salitre hacia los puertos, mientras que el Estado invertía en la consolidación de su presencia en el centro y sur del país (Moraga Feliú, 2013).

Treinta y tres años más tarde de aquel hito, el 4 de enero de 1884, el presidente de la República, Domingo Santa María, firmó un decreto que estableció la Empresa de

---

<sup>7</sup> La contenedorización es un método logístico que utiliza contenedores estandarizados para facilitar el transporte y almacenamiento de mercancías en diferentes modos, como marítimo, terrestre y ferroviario. Este sistema mejora la eficiencia, reduce costos y optimiza la manipulación de cargas.

los Ferrocarriles del Estado (EFE), reconociendo la importancia estratégica del ferrocarril para el desarrollo del país<sup>8</sup>. Este decreto unificó la explotación de la mayoría de los servicios ferroviarios privados existentes en Chile<sup>9</sup>. La nueva empresa se configuró como un servicio público de propiedad estatal, encargada de desarrollar, promover y gestionar los servicios de transporte ferroviario tanto de pasajeros como de carga<sup>10</sup> (Empresa de Ferrocarriles del Estado, 2024).

Tras el triunfo de Chile en la Guerra del Pacífico, el presidente José Manuel Balmaceda, con una clara visión estratégica, impulsó las bases que llevaría a unir el país por ferrocarril desde Iquique hasta Puerto Montt, estableciendo lo que se convertiría en la columna vertebral del país. Esta infraestructura clave, permitiría integrar los amplios territorios del norte, donde la comunicación marítima no contaba con la rapidez necesaria para trasladar urgentemente un contingente militar a estas tierras para ejercer soberanía, de manera que el impulso del proyecto, no solo facilitaría la conexión territorial, sino que también fortaleciera la cohesión nacional y la seguridad del país (Memoria Chilena, 2024).

El reto de anexar el norte con el centro y sur del país no era una empresa fácil. A principios del siglo XX, la longitud de la red ferroviaria nacional era de 3.981 km, los cuales 2.317 km. pertenecía a ferrocarriles particulares, provenientes principalmente del norte del país, ligados a la industria minera y salitrera (Marín Vicuña, 1901). Estos ferrocarriles venían desde el interior hacia la costa, en trayectos conocido como “ramal”. En cambio, la red sur estaba compuesto mayoritariamente por medios estatales conectados por la estratégica línea férrea “Longitudinal”. La conexión no estaría exenta de escollos, producto que la explotación del ferrocarril en el norte no coexistió una visión de integración a futuro, siendo una construcción de infraestructura ferroviaria inorgánica reflejada en los diferentes anchos de vía o trochas ocupadas en ese entonces, siendo incompatible varios tramos entre sí.

---

<sup>8</sup> El desarrollo del ferrocarril fue una proyección estratégica para superar el aislamiento y la falta de comunicación en las regiones más distantes, permitiendo una administración más efectiva y permitir al Estado ejercer control efectivo en todo el territorio. Con la llegada del tren, las distancias se acortaron y los viajes se volvieron seguros, económicos y accesibles, facilitando así el transporte de personas y mercancías. La expansión de los trenes promovió la integración y un sentido de pertenencia compartida en Chile, contribuyendo a una visión colectiva del futuro.

<sup>9</sup> Como resultado, se integraron bajo una sola administración las compañías que operaban el Ferrocarril de Santiago a Valparaíso, el Ferrocarril del Sur, que conectaba Santiago con Curicó, y el Ferrocarril de Talcahuano, que iba de Curicó a Angol.

<sup>10</sup> Con la creación de la estatal, el ferrocarril tuvo un crecimiento exponencial, especialmente entre 1880 y 1930, periodo en el que alcanzó su máximo esplendor, manteniendo un rol protagónico hasta la década de 1960.

Desde el punto de vista estratégico, aparecen estudios militares sobre el uso del ferrocarril en la movilización y concentración de fuerzas. El estudio sobre la defensa territorial de Chile elaborado por el Capitán del Estado Mayor General, F.J. Díaz, y publicado en la primera edición del Memorial del Ejército en 1906, exponía sobre lo indispensable de contar con la extensión de la línea férrea longitudinal hacia el norte, ya que a principios de siglo no existía conexión hacia el área septentrional del país. Este estudio destacaba la conveniencia que tendría para la defensa del país contar con esta vía longitudinal y la exigencia de contar con la infraestructura que pudiera entregar la movilidad estratégica necesaria para la concentración y movilización del Ejército y la Armada.

### **Ferrocarril Militar del Ejército de Chile**

Dada la importancia en la explotación y operación del ferrocarril por parte del Ejército por temas estratégicos y de seguridad, el Estado cedió la administración del tramo Puente Alto a El Volcán al Batallón de Ferrocarrileros N°1 del “General Alberto Herrera”, que lo operó bajo una regulación dictada por el Ministerio de Ferrocarriles<sup>11</sup> para su mantenimiento y explotación (Ejército de Chile, 1934). El ferrocarril quedó bajo la responsabilidad del comandante del Batallón de Ferrocarrileros. Esta unidad se encargaba de la operación y mantenimiento, debiendo generar suficientes ingresos para autofinanciarse, lo que se logró en las primeras décadas, situación que se deterioró con el tiempo. El ferrocarril mantuvo un nivel de éxito relativamente alto en comparación con otros ramales de características similares (Vargas, 2024).

El ferrocarril militar tuvo el propósito de mantener capacitado al Ejército en la operación de ferrocarriles, siendo su función principal la de garantizar la práctica del personal militar pensando en eventuales emergencias nacionales y proporcionar protección estratégica en los pasos cordilleranos (Thompson & Angerstein, 2000). En 1937, quedó reflejado su capacidad y nivel de entrenamiento al construir un trecho de 18 km que separa a la Escuela de Aviación "El Bosque" y la estación de campaña en un tiempo de 8 días, siendo destacado por las autoridades de la época (Ejército de Chile, 1937).

---

<sup>11</sup> Considerando la necesidad de procurar la instrucción práctica al personal del Cuerpo de Ferrocarriles, por decreto N.º 129, de 20 de Abril de 1913, del Ministerio de Ferrocarriles, dispuso que la explotación del Ferrocarril quedara a cargo del comandante del Batallón de Ferrocarrileros, en las siguientes condiciones: entrega bajo inventario, itinerario, tarifas, reglamentos, y presupuestos de gasto sometidos a la aprobación del Ministerio de Ferrocarriles, así como posteriormente por el Estado Mayor del Ejército, el Ministerio de Obras Públicas y la Empresa de Ferrocarriles del Estado.

Varios factores llevaron al cierre del tramo, por una parte, a partir de 1950, el ferrocarril en Chile, como en resto del mundo, comenzó a perder competitividad frente al transporte vehicular y aéreo debido al crecimiento del parque automotor<sup>12</sup> y la falta de inversiones en su infraestructura. Los terremotos, los problemas de mantenimiento y la reducción en los volúmenes de carga transportados, jugaron un papel crucial en esta disminución. El ferrocarril se cerró en 1964 y con ello el comienzo de un declive generalizado en el sistema ferroviario nacional, agravado en la década de 1980, cuando se implementó una política de autofinanciamiento, eliminando los subsidios que limitaron su capacidad de funcionamiento (Empresa de Ferrocarriles del Estado, 2024).

### **Figura N° 1**

*Batallón Ferrocarrilero en labores de mantención y reparación de infraestructura ferroviaria*



*Nota:* Los Ferrocarrileros Fuente: Zig-Zag: año IX, números 465-475, 17 de enero a 28 de marzo de 1914 <https://www.flickr.com/photos/stgonostalgico/52713724606>

---

<sup>12</sup> Entre 1950 y 1995, el número de vehículos aumentó de 472,000 a más de 1.6 millones, y la red vial se expandió significativamente.

## **Figura N° 2**

### *Compañía de Tren N°2*



*Nota:* Carga equipos previo a la salida a maniobras el 2 de abril de 1910. Fuente: Academia de Historia Militar <https://www.academiahistoriamilitar.cl/academia/compania-de-tren-n2-2/>

## **La importancia de la movilidad estratégica en Europa**

Desde el inicio de la guerra ruso – ucraniana en 2022, el ferrocarril ha tenido un desempeño fundamental en la logística militar de ambos bandos, recuperando la notoriedad e importancia que tuvo hasta la IIGM. En este conflicto ha quedado demostrado por ejemplo la dependencia de la logística rusa en los ferrocarriles, la que se desarrolló en el antiguo espacio soviético, donde tanto el Imperio ruso como la Unión Soviética fomentaron el impulso de una extensa red ferroviaria.

En esta guerra, Rusia ha ejecutado su invasión empleando extensos recursos, principalmente de vehículos acorazados que han debido transportarse desde la profundidad de su vasto territorio. El abastecimiento de las fuerzas rusas se ha utilizado en gran medida en la conexión ferroviaria entre el Cáucaso y Crimea. Sin embargo, la ruta presenta un desvío significativo, obligando a Rusia a recurrir al transporte por carretera, que carece de la capacidad logística del ferrocarril y que, en cierta forma, la poca diversificación en el transporte ruso ha presentado un obstáculo logístico importante.

Conjuntamente, el intento por parte de Ucrania de interrumpir las rutas de suministro en múltiples ocasiones ha presentado dificultades para la logística ferroviaria rusa. Los ucranianos han llevado a cabo variados sabotajes en las vías del sur, atacando

infraestructuras estratégicas desde el aire, como el puente de Crimea. A pesar de estos ataques, las fuerzas rusas han logrado mantener la operatividad de su red ferroviaria, utilizando unidades especializadas y trenes blindados para la vigilancia y el mantenimiento de las infraestructuras críticas que demuestra la resiliencia de la red ferroviaria rusa (Latschan, 2022).

Asimismo, la red ferroviaria de Ucrania también ha tenido un rol crucial en el contexto de la guerra, transformándose en la principal empresa logística del país. Con aproximadamente 23,000 kilómetros de vías y 400,000 empleados, los ucranianos cuentan con un sistema ferroviario relativamente moderno, erigiéndose como un símbolo de resistencia, encargado del transporte de armamento, ayuda humanitaria y la evacuación de millones de personas que huyen de los combates. Además, están facilitando el regreso de familias a áreas previamente ocupadas por tropas rusas. Junto con lo anterior, Ucrania ha intensificado el uso del ferrocarril para exportar productos como trigo, carbón y acero hacia países occidentales, producto del bloqueo del puerto de Odesa por parte de Rusia, siendo un medio esencial para aliviar la economía ucraniana. Sin embargo, la guerra ha causado daños significativos en la infraestructura ferroviaria. Los constantes bombardeos rusos han obligado a la red ferroviaria a implementar rutas de desvío. A pesar de estos desafíos, la red continúa operando (De Moya Martínez, 2024).

La guerra en Ucrania ha puesto de manifiesto la crucial necesidad de una movilidad estratégica efectiva en Europa. La agresión rusa ha revelado importantes deficiencias en el sistema de transporte europeo, especialmente en relación con las conexiones hacia Ucrania. Para lo anterior, es esencial que la red TEN-T<sup>13</sup>, en particular los corredores de la malla principal, esté diseñada para uso civil como militar. Esto implica la modernización de la infraestructura para facilitar el transporte de material militar pesado cuando sea necesario (Rúa, 2022).

La agresión militar de Rusia en la frontera este de Europa ha acusado la importancia de la cooperación continua entre la Unión Europea (UE) y la OTAN para establecer normas y procedimientos que fortalezcan los convoyes militares a lo largo de la red TEN-T durante tiempos de paz, crisis y guerra. La estrategia debe aprovechar el efecto de la red ferroviaria para permitir movimientos céleres, incluso cuando algunos tramos no estén totalmente operativos. Para ello, es fundamental desarrollar y mantener suficientes rutas alternativas que proporcionen redundancia y fortalezcan la resiliencia de toda la red férrea.

---

<sup>13</sup> Las Redes Transeuropeas de Transporte (RTE-T), conocidas en inglés como Trans-European Transport Networks (TEN-T), constituyen un conjunto de redes prioritarias de transporte diseñadas por la Dirección General de Movilidad y Transportes (DG MOVE) de la Comisión Europea. Su objetivo es facilitar la movilidad de personas y mercancías en toda la Unión Europea (UE).

La movilidad estratégica se ha convertido en una prioridad dentro de la política de transportes de la UE, lo que presenta un nuevo desafío: la necesidad de acelerar la conexión de sus principales puertos con el ancho de vía internacional. Esto es crucial para poder enviar tropas, material militar y otros suministros al este de Europa en caso de emergencia. La reciente agenda en Bruselas ha destacado la importancia de la movilidad estratégica, especialmente en las reuniones sobre los corredores ferroviarios europeos.

Las redes ferroviarias de varios países presentan un problema significativo debido a que se construyeron con diferentes anchos de vía. Mientras que la red en la Península Ibérica utiliza el ancho de 1668 milímetros, países como Ucrania y las repúblicas bálticas operan con el ancho ruso de 1520 milímetros. Esta discrepancia limita la capacidad de actuar como una retaguardia eficaz en un conflicto que involucre a la OTAN. Actualmente, Barcelona es el único nodo en la península ibérica que puede enviar convoyes militares a la red europea sin problemas de ancho de vía, lo que la convierte en un punto estratégico clave para la OTAN.

Asimismo, la revalorización de la movilidad estratégica ha impulsado la industria que posee la tecnología para construir trenes capaces de operar en distintos anchos de vía<sup>14</sup>, facilitando así la conexión entre las infraestructuras ferroviarias europeas y rusas.

## **Conclusiones**

La movilidad estratégica se ha definido como un pilar esencial para la efectividad de las operaciones militares modernas, enmarcando la capacidad de trasladar unidades y recursos a teatros de operaciones. Este concepto no solo es relevante a nivel nacional, sino que también están presentes en las estrategias de organizaciones internacionales como la OTAN. La posibilidad de desplazar fuerzas a grandes distancias de manera rápida y eficiente se convierte en una necesidad crítica en un mundo en constante cambio y conflicto.

La historia demuestra que el ferrocarril ha sido un medio clave en la movilización de tropas y abastecimientos, desde la Guerra Civil estadounidense hasta la actualidad,

---

<sup>14</sup>Ancho Variable de Mercancías (OGI) es un sistema ferroviario que adapta el ancho de los ejes de los vagones para facilitar su circulación en redes con diferentes anchos de vía. Este sistema elimina la necesidad de transbordos al cruzar fronteras, lo que reduce el tiempo de tránsito y costos operativos. Con ejes ajustables, los trenes pueden operar eficientemente en diversas redes, optimizando el transporte de mercancías y mejorando la conectividad entre regiones (Tren online, 2024).

donde ha recuperado su importancia en la guerra en Ucrania. La utilización del ferrocarril permite superar las limitaciones logísticas que otros modos de transporte no pueden proporcionar, especialmente en contextos de emergencia. Por lo tanto, la infraestructura ferroviaria debe estar adaptada para usos tanto civiles como militares, asegurando que la movilidad estratégica se mantenga como una prioridad.

### **Figura N° 3**

*Leopard 2E embarcado en ferrocarril*



Nota: Tanque Leopard 2E del Ejército de Tierra Español, siendo estibado por personal especialista.

Fuente: Sin perder el Tren. Revista Española de Defensa, abril 2022.

<https://working.mde.es/Galerias/gabinete/red/2022/04/p-30-35-red-393-ferroviarios.pdf>

La guerra en Ucrania ha evidenciado las deficiencias en las redes de transporte europeo y ha subrayado la importancia de una colaboración robusta entre la Unión Europea y la OTAN para adaptar la infraestructura existente a las exigencias contemporáneas. El desarrollo de corredores logísticos eficientes y la creación de alternativas robustas son vitales para garantizar que las fuerzas militares puedan actuar con rapidez y efectividad.

Frente a estos desafíos, se debe afrontar la necesidad de actualizar las conexiones ferroviarias para alinearse con estándares internacionales. La discrepancia en los anchos de vía entre diferentes países representa un obstáculo significativo que limita la capacidad de respuesta ante crisis.

Para Chile, la historia del ferrocarril revela una necesidad imperante de mantener y restaurar una infraestructura ferroviaria que maximice su potencial estratégico. Aunque el sistema ferroviario chileno ha enfrentado desafíos en su historia, su revalorización es esencial en un contexto militar actual donde se requiere agilidad y efectividad en la movilización de tropas. La visión estratégica en el transporte son pasos necesarios para garantizar que Chile esté preparado para afrontar cualquier eventualidad, colaborando estrechamente con todos los actores del sistema ferroviario.

Finalmente, la importancia de la movilidad estratégica y el ferrocarril se ha reafirmado en la actualidad, destacando la necesidad de integrar y modernizar las infraestructuras ferroviarias para los desafíos de un mundo cambiante. Los esfuerzos concertados de los países europeos y la colaboración con organizaciones como la OTAN son imprescindibles para garantizar la seguridad y la capacidad de respuesta ante posibles crisis de seguridad en el futuro.

## Referencias

- Barclay, C. (20 de 04 de 2024). *Helmuth von Moltke*. Encyclopedia Britannica: <https://www.britannica.com/biography/Helmuth-von-Moltke>
- De Moya Martínez, M. (9 de enero de 2024). *Descifrando la Guerra*. Mapa de la logística ferroviaria rusa en el sur de Ucrania: <https://www.descifrandolaguerra.es/mapa-de-la-logistica-ferroviaria-rusa-en-el-sur-de-ucrania>
- Derrick, B. (08 de septiembre de 2011). *The National Archives*. <https://media.nationalarchives.gov.uk/index.php/railways-and-the-mobilisation-for-war-in-1914/>
- Ejército de Chile. (1934). *Reglamento Interno del Ferrocarril Militar de Puente Alto al Volcán*. Instituto Geográfico Militar.
- Ejército de Chile. (1937). Ferrocarril Militar entre Puente Alto y El Bosque. En *Memorial del Ejército de Chile*. Estado Mayor del Ejército.
- Ejército de Chile. (2011). *Conducción de la Fuerza Terrestre en un Teatro de Operaciones Conjunto*. División Doctrina.
- Empresa de Ferrocarriles del Estado. (12 de septiembre de 2024). *EFE Trenes de Chile*. <https://www.efe.cl/corporativo/historia/#:~:text=1851%20%E2%80%93%20Primer%20Tren%20en%20Chile,incipiente%20red%20ferroviaria%20de%20Chile>.
- Evenson, J. (2006). *Capability in Decline: A Historical Analysis of the Post-Wold War II Degradation of Domestic Railroads and The Impact on the Unites States Military*. Faculty of the United States Army Command and General Staff College.
- G.G. Lepage, J.-D. (2017). *Military Trains and Railways*. McFarland & Company, Inc., Publishers.
- Hernández Tortajada, F. (1999). La Proyección de Fuerzas: El Transporte Estratégico. En CESEDEN, *Boletín de Información* (págs. 55-65).
- Imperial War Museums. (16 de 09 de 2024). *Imperial War Museums*. <https://www.iwm.org.uk/history/transport-and-supply-during-the-first-world-war>
- Joint Chiefs of Staff. (2020). *Joint Planning*. Joint Publication 5-0.
- Latschan, T. (05 de mayo de 2022). *Deutsche Welle*. Los ferrocarriles de Ucrania, un factor clave en la guerra: <https://www.dw.com/es/los-ferrocarriles-de-ucrania-son-un-factor-clave-en-la-guerra/a-61700214>

- Marín Vicuña, S. (1901). *Estudios de los Ferrocarriles Chilenos*. Imprenta Cervantes.
- Memoria Chilena. (17 de agosto de 2024). *Memoria Chilena*. <https://www.memoriachilena.gob.cl/602/w3-article-97337.html>
- Ministerio de Defensa Nacional. (2014). *DNC 4-0 Doctrina Logística para el Empleo Conjunto de la Fuerza*. Doctrina Nacional Conjunta.
- Moraga Feliú, P. (2013). *TIEMPO DE TRENES Imaginario del Ferrocarril en Chile. 1860 - 1960*. Librería Editorial Ricaaventura EIRL.
- Network Rail. (12 de noviembre de 2021). *Film: The Railway at War – 1939-1945*. <https://www.networkrail.co.uk/stories/film-the-railway-at-war-1939-1945/>
- Rúa, C. (6 de octubre de 2022). *PierNext*. La Red Transeuropea de Transporte se extiende hacia el Este: <https://piernext.portdebarcelona.cat/movilidad/la-red-de-transporte-transeuropea-se-extiende-hacia-el-este/>
- Smithsonian Institution. (febrero de 2015). *How the Railroad Won the War*. <https://americanexperience.si.edu/wp-content/uploads/2015/02/How-the-Railroad-Won-the-War.pdf>
- Thompson, I., & Angerstein, D. (2000). *Historia del Ferrocarril en Chile*. Ediciones de la Dirección de la Bibliotecas, Archivos y Museos.
- Thomson, I., & Angerstein, D. (2000). *Historia del Ferrocarril en Chile*. Ediciones de la Dirección de Bibliotecas, Archivos y Museos.
- Tren online. (15 de agosto de 2024). *Eje de Ancho variable para mercancías*. <https://www.revistatren.com/noticias/220-pruebas-en-via-del-eje-de-ancho-variable-para-mercancias>
- Vargas, E. (22 de agosto de 2024). *Amigos del Tren*. <https://www.amigosdeltren.cl/historia-del-fc-de-puente-alto-a-el-volcan#:~:text=Este%20peque%C3%B1o%20ferrocarril%20con%20una,2.335.630%20pesos%20de%20oro>.