FUNDADO EL 15 DE JULIO DE 1906

ISSN Nº 0716-3835

MEMORIAL

DEL

Ejército de Chile

CENTRO DE ESTUDIOS E INVESTIGACIONES MILITARES
MARZO - 2019 Nº 502

FUNDADO EL 15 DE JULIO DE 1906

MEMORIAL
DEL
Ejército de Chile

CENTRO DE ESTUDIOS E INVESTIGACIONES MILITARES

MARZO - 2019 Nº 502

IMPRESO EN LOS TALLERES DEL INSTITUTO GEOGRÁFICO MILITAR
INSCRIPCIÓN Nº 92.946

Centro de Estudios e Investigaciones Militares
Bandera 52, Santiago - Chile
Teléfonos: (56-2) 226683800 - 226683836
ISSN Nº 0716-3835

MEMORIAL DEL Ejército de Chile

Nº 502 - MARZO 2019

EDITORIAL

MEMORIAL
DEL
Ejército de Chile

EDITORIAL

En este nuevo año, presentamos con innegable alegría una nueva edición del Memorial del Ejército de Chile, dedicada en esta oportunidad a los ganadores del concurso de artículos militares, organizado por la institución el año recién pasado.

Considerando la necesidad de incentivar los procesos de investigación y desarrollo, vinculados a los requerimientos que la institución posee en dicho aspecto, se llevó a efecto el concurso "Desarrollando Capacidades Militares", cuyas bases fueron difundidas a toda la institución.

A través de él, se buscó recibir todas las ideas e iniciativas que pudieran ser aplicadas y/o estudiadas, para beneficiar las capacidades del Ejército, entendidas estas como los recursos o aptitudes para desarrollar sus actividades, en todos los ámbitos de su responsabilidad.

El desarrollo del concurso recayó en el Centro de Estudios e Investigaciones Militares (CESIM), en el marco del Sistema de Investigación y Desarrollo del Ejército (SIDE).

Participaron 97 integrantes de la institución, incluyendo personal en retiro y reservistas del Ejército.

Se pretendía que los trabajos dieran origen a procesos de investigación y desarrollo, con temas de libre elección del concursante, relacionados con los cuatro ámbitos del Sistema de Investigación y Desarrollo del Ejèrcito y sus respectivas áreas, los que se señalan a continuación:

- ✓ Ámbito seguridad y defensa.
- ✓ Ámbito de ciencia y tecnología.
- ✓ Ámbito de recursos humanos y estudios sociales.
- ✓ Ámbito de ciencias militares, combate, generación de doctrina y docencia.

Los resultados, en términos de participación y calidad de los trabajos, como asimismo, en cuanto a la profundidad, interés y variedad de temas fueron sobresalientes, por lo que constituye un deber agradecer a través de las presentes líneas, la contribución de los autores.

Como es lógico, no es posible reflejar en el presente Memorial todos los artículos presentados, por lo que, por decisión editorial, se han seleccionado los artículos premiados con los tres primeros puestos, en los ámbitos mencionados.

En futuras ediciones de nuestra revista y en otras publicaciones militares, se darán a conocer otros artículos, de tal forma de difundirlos al personal de la institución. Independiente de ello,

todos los artículos están siendo analizados por los respectivos ámbitos, para determinar su aprovechamiento institucional.

Las temáticas que aparecen en la presente edición, enmarcadas como ya ha sido dicho en los ámbitos ya mencionados, abarcan temas como: "Computación cuántica y sus potenciales implicancias para la defensa", "Modelos de predicción para proyectiles y su desarrollo a través de uso de algoritmos", "Primera detección de CRYPOSPORIDIUM SP, parásito intestinal en mariscos destinados a consumo humano en Chile" y "Diseño y desarrollo de una plataforma colaborativa para el control de unidades civiles y militares de emergencia".

Finalmente, queremos testimoniar el apoyo al proceso llevado a cabo en el concurso, por parte de los cuatro ámbitos de investigación y desarrollo del Ejército, cuyas responsabilidades recaen en el Centro de Estudios e Investigaciones Militares en el caso de seguridad y defensa, Comando de Industria Militar e Ingeniería para ciencia y tecnología, Comando General del Personal en lo referido a recursos humanos y estudios sociales y Comando de Educación y Doctrina en cuanto a ciencias militares, combate, generación de doctrina y docencia.

SEGURIDAD Y DEFENSA

MEMORIAL
DEL
Ejército de Chile

COMPUTACIÓN CUÁNTICA Y SUS POTENCIALES IMPLICANCIAS PARA LA DEFENSA[1]

MAYOR CRISTIÁN BARRÍA HUIDOBRO[2]

Resumen: *la computación cuántica ha sido un foco de atención para investigadores durante los últimos años. En teoría, el potencial de esta tecnología incluye la capacidad de permitir el acceso a los principales métodos de criptografía basados en las llaves públicas actualmente existentes, las que son usadas indistintamente en ámbitos civiles y militares. Combinando ambas, la criptografía cuántica parece ser una alternativa a este problema. En el presente documento se abordan estos conceptos, y se analizan los potenciales efectos que pueden tener en las tecnologías usadas actualmente en el país.*
Palabras clave: *computación cuántica, criptografía cuántica, criptografía poscuántica, ciberseguridad.*

Abstract: *quantum computing has been a focus of attention during the last years. In theory, the potential of this technology includes the capacity of breaking all the main public key based on the encryption methods currently existing, which are used in both civil and military areas. In this context, quantum cryptography may be an alternative to this issue. This paper approaches those concepts, and analyzes the potential effects that might affect the technologies currently used in the country.*
Keywords: *quantum computing, quantum cryptography, posquantum cryptography, cybersecurity.*

INTRODUCCIÓN

La computación cuántica permite la realización de operaciones de manipulación y almacenamiento de datos, mediante el uso intencional y dirigido, de fenómenos cuánticos. Desde la primera propuesta de algoritmos especialmente diseñados para su aplicación en este tipo de computación, la investigación relacionada con este campo ha venido en aumento.

La capacidad de realizar complejas operaciones de cómputo en tiempos mucho menores que los usualmente posibles para la computación clásica, permite a la computación cuántica tener

1 Artículo ganador del primer puesto del concurso "Desarrollando Capacidades Militares", en el ámbito de seguridad y defensa.
2 Doctor en ingeniería informática, Magíster en ciencias de la ingeniería informática y Magíster en planificación y gestión educacional, Licenciado en informática y Licenciado en ciencias de la ingeniería.

un amplio espectro de aplicaciones, incluyendo medicina, finanzas, entre otros. En el presente artículo nos enfocaremos en una de estas aplicaciones, dada su relevancia para la ciberseguridad nacional y la defensa: la criptografía cuántica.

El desarrollo del presente artículo, considera una introducción, seguido de una primera parte en donde se proveen trabajos relacionados sobre la computación cuántica y la criptografía cuántica. La segunda detalla los trabajos actuales de cifrado cuántico y cifrado poscuántico. La tercera parte consta de un análisis simple de ciertas tecnologías empleadas en Chile, junto con observaciones sobre las posibles implicancias acerca del uso de la computación cuántica contra esas tecnologías. Finalmente, se entregan las conclusiones.

TRABAJOS RELACIONADOS

Computación cuántica

La computación cuántica es aquella que utiliza los fenómenos físicos de la mecánica cuántica para realizar operaciones de cómputo.[3] Es decir, se entiende como computador cuántico al dispositivo que realiza dichas operaciones, basado en las dinámicas de objetos a nivel atómico, como por ejemplo, partículas de dos estados con el fin de almacenar y manipular datos.[4] Si bien la aplicación de los fenómenos de la mecánica cuántica no es un concepto nuevo, su importancia para la criptografía cobró verdadera implicancia cuando Shor expuso sus algoritmos cuánticos para factorizar y computar logaritmos discretos, momento en el que quedó en evidencia que la criptografía, en base a llaves públicas, podía ser vencida con computadores cuánticos.[5]

Dentro de los diferentes efectos físicos de la mecánica cuántica que son explorados para su aplicación en la computación, destaca el entrelazamiento cuántico, el que se entiende como una noción especial de la superposición cuántica y permite la ejecución de múltiples operaciones de cómputo de forma simultánea, empleando las mismas unidades elementales de los recursos de un sistema. Esto se traduce en la capacidad de los computadores cuánticos para realizar grandes y complejas tareas de cómputo, en un tiempo exponencialmente menor si se compara con los computadores clásicos.[6] Un aumento de tal magnitud en el poder de cómputo implica que diversas

3 GERSHENFELD, N., & CHUANG, I. (1998). Quantum Computing with Molecules. *Scientific American, 278*(6), 66-71. Retrieved from http://www.jstor.org/stable/26057857

4 SPECTOR, Lee; BARNUM, Howard; BERNSTEIN, and Nikhil SWAMY, Herbert J. (1999). Quantum computing applications of genetic programming. In *Advances in genetic programming,* SPECTOR, Lee; LANGDON, William B.; O'REILLY, Una-May and ANGELINE, Peter J. (Eds.). MIT Press, Cambridge, MA, USA, pages 135-160.

5 SHOR, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Symposium on Foundations of Computer Science,* (1994) pages 124–134.

6 JOZSA, R. (1997). Entanglement and quantum computation. *arXiv preprint quant-ph/9707034*.

tareas de Big Data, inteligencia de negocios, análisis matemáticos y estadísticos, entre otros, puedan realizarse de forma mucho más eficiente. Es sencillo proyectar los beneficios que esto puede significar para las instituciones de defensa, las que podrían contar con los resultados que esperan de sus análisis de datos mucho más rápido, facilitando, además, la toma de decisiones e incluso cuando se consideran grandes cantidades de datos. Labores de análisis de datos de geolocalización, de bases de datos, inteligencia y cualquier otra operación de alta exigencia computacional podrá traducirse en acciones concretas mucho más rápido. Proyectos de inteligencia artificial y aprendizaje de máquina también se verán beneficiados por este tipo de tecnologías.[7]

Criptografía cuántica

Si bien los detalles físicos de la criptografía cuántica están fuera del alcance de este documento, es importante conocer que una parte significativa de la criptografía cuántica se basa en el principio de incertidumbre de Heisenberg[8] y el teorema de no-clonación propuesto por Wootters y Zurek,[9] el que fue demostrado por Dieks.[10] De manera simple se puede explicar que el principio de incertidumbre de Heisenberg sostiene que la simple observación de un elemento cuántico cambia su comportamiento.

Por otro lado, el teorema de no-clonación declara que es imposible crear una copia exacta de un estado cuántico desconocido. Para ilustrar de forma simple la relevancia de estos efectos, esto significa que un mensaje cuántico, enviado desde A hasta B, se vería inmediatamente afectado si un actor C intentara mirar su contenido. De este modo, tanto A y B podrían saber rápidamente que existe alguien que está intentando interceptar la comunicación.

Las ventajas de un sistema de comunicación así son evidentes, especialmente en el contexto de las comunicaciones confidenciales a nivel militar. Es por esto que la computación cuántica y la encriptación cuántica ofrecen herramientas potentes tanto para acceder (romper en jerga informática) los sistemas de criptografía clásicos, en base a llaves públicas, como también para establecer comunicaciones confidenciales. En general, un actor cuyo sistema de encriptación se basa en la computación clásica puede, teóricamente, ser vencido fácilmente por un adversario que posee herramientas de computación cuántica. Alternativas ampliamente usadas como Rivest, Shamir and Adleman (RSA), Digital Signature Algorithm (DSA) y Elliptic Curve Digital Signature

7 IBM Q (2018). Applications of quantum computing. IBM. Fuente: https://www.research. ibm.com/ibm-q/learn/quantum-computing-applications/

8 HEISENBERG, W. (1985). Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. In: BLUM, W.; RECHENBERG, H., DÜRR, HP. (eds) *Original Scientific Papers Wissenschaftliche Originalarbeiten.* Werner Heisenberg Gesammelte Werke Collected Works, vol A / 1. Springer, Berlin, Heidelberg

9 WOOTTERS, W. and ZUREK, W. *Physics Today* 62, 2, 76 (2009); doi: 10.1063/1.3086114.

10 DIEKS, D. Communication by EPR devices, Physics Letters A, Volume 92, Issue 6, 1982, Pages 271-272, ISSN 0375-9601, https://doi.org/10.1016/0375-9601(82)90084-6. (http://www. sciencedirect.com/science/article/pii/0375960182900846)

Algorithm (ECDSA) pueden ser quebradas por la computación cuántica, implicando un riesgo de seguridad tanto para entornos civiles como militares.

No obstante, es importante conocer que la criptografía también ofrece otras técnicas, como la criptografía basada en código, la que se origina desde ecuaciones cuadráticas multivariable, que se cree que resisten tanto medios de computación clásica como cuánticos.[11] La capacidad de resistencia de estas alternativas que emplean computación cuántica se basa en que, en la actualidad, no se han encontrado ataques efectivos contra dichas alternativas, por lo que la computación cuántica no ofrece una mejora o potencial solución.[12] Pero, esto no garantiza que un ataque no sea descubierto a futuro, y, por ende, optimizado por el uso de la tecnología cuántica.

Criptografía cuántica y criptografía poscuántica

El potencial que puede adquirir un adversario con acceso a la computación cuántica ha impulsado el presente artículo, con el propósito de identificar sistemas criptográficos que sean capaces de enfrentar ataques con dicha tecnología, dando paso a lo que se conoce como criptografía poscuántica. Este escenario debiese ser estudiado en profundidad por las instituciones de defensa, por cuanto es cuestión de tiempo hasta que este tipo de tecnología se aplique de forma práctica, se masifique y se encuentre en manos de potenciales adversarios. Sin ir más lejos, el National Institute of Standards Thecnology (NIST) proyecta contar con un borrador de sus estándares para criptografía poscuántica para los años 2022 a 2024.[13] Perlner *et al*. (2009), provee de una exhaustiva revisión de algoritmos resistentes al uso de tecnologías cuánticas, mientras que Bernstein (2009), argumenta las alternativas que ofrece la criptografía para enfrentar un escenario con atacantes que disponen de tecnología cuántica. La literatura evidencia que este tema está siendo abordado activamente por la comunidad internacional, por lo cual, será importante para el país que las instituciones de defensa consideren optar por un rol proactivo en el estudio, desarrollo y aplicación de estas tecnologías. Esto con el fin de evitar vulnerabilidades relacionadas con desventaja tecnológica ante potenciales adversarios.

Tecnologías empleadas en Chile

Si bien obtener un catastro detallado de las tecnologías relacionadas con las comunicaciones y, particularmente, aquellas relacionadas con sistemas criptográficos en la defensa no es razonablemente posible (y si lo fuera, sería preocupante), si se puede obtener una mirada superficial basándose en los sistemas operativos (SO) que son utilizados por distintos integrantes de las

11 BERNSTEIN, D. J. (2009). Introduction to post-quantum cryptography. In *Post-quantum cryptography* (pp. 1-14). Springer, Berlin, Heidelberg.

12 PERLNER, R. A., & COOPER, D. A. (2009, April). Quantum resistant public key cryptography: a survey. In *Proceedings of the 8th Symposium on Identity and Trust on the Internet* (pp. 85-93). ACM.

13 Computer Security Resource Center (2018). Post-Quantum Cryptography: Workshops and Timeline. Information Technology Laboratory (ITL), National Institute of Standards and Technology (NIST). Fuente: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

instituciones de defensa. En general, se puede identificar el uso de tres de los SO más populares (Microsoft Windows, Mac OS y Ubuntu Linux) en los equipos de escritorio, y el uso de iOS y Android en dispositivos móviles. Si bien cada SO permite el uso de herramientas creadas por terceros, esto puede implicar riesgos importantes de seguridad, por lo cual se presume la ausencia de este tipo de herramientas; salvo en casos de excepciones debidamente analizados, que pueden ocurrir al operar con proveedores externos de tecnologías.

Es común que, para acceder de manera segura (fiable) a servidores y otros equipos computacionales, se utilice Signal Shell (SSH), para lo cual existen herramientas ampliamente usadas, que se apoyan en RSA para la ejecución de sus tareas criptográficas,[14] incluso para distintos SO.[15] Sumado a las vulnerabilidades propias de cada SO (especialmente aquellos de dispositivos móviles), es claro que la confidencialidad de la información se ve amenazada por ataques tanto clásicos como cuánticos, pero estos últimos alcanzarían sus objetivos de forma mucho más rápida. Por tanto, el potencial daño que pueda ocasionar un ataque de este tipo es mayor, ya que el atacante cuenta con más opciones para obtener información sensible, tales como contraseñas y otros. Y esto solo es un ejemplo particular. Muchas otras tecnologías pueden evaluarse, exponiendo el riesgo al que están expuestos los sistemas actualmente en uso.

DISCUSIÓN Y CONCLUSIONES

La computación cuántica está en constante desarrollo, por lo cual es esperable que en un futuro relativamente cercano se alcance el punto en el cual los sistemas criptográficos de llave pública, como RSA, pasen a la obsolescencia. Esta situación, lejos de ser una amenaza, supone una oportunidad para la defensa, permitiendo realizar un análisis crítico de las tecnologías que deben ser reemplazadas, particularmente aquellas que presten servicios a componentes críticos y/o sensibles de las distintas instituciones. Además, el desarrollo de la criptografía poscuántica representa el siguiente nivel en lo que a protección de la confidencialidad e integridad en las comunicaciones respecta. Finalmente, el potencial de realizar rápidamente cálculos complejos, que normalmente requerirían meses de procesamiento, implica que la computación cuántica también puede ser una herramienta de utilidad para realizar análisis sobre grandes cantidades de datos, lo cual agiliza, por ejemplo, labores de inteligencia, optimizaciones, simulaciones, entre otras.

BIBLIOGRAFÍA

GERSHENFELD, N., & CHUANG, I. (1998). Quantum *Computing* with Molecules. *Scientific American,* 278(6), 66-71. Retrieved from http://www.jstor.org/stable/26057857

14 SSH (2018). PuTTYgen - Key Generator for PuTTY on Windows. SSH.com. Fuente: https://www.ssh.com/ssh/putty/windows/puttygen

15 SSH (2018). Puttygen on Linux - SSH Key Generator. SSH.com. Fuente: https://www.ssh.com/ssh/putty/linux/puttygen

SPECTOR, Lee; BARNUM,Howard; BERNSTEIN, Herbert J. and SWAMY, Nikhil (1999). Quantum computing applications of genetic programming. In *Advances in genetic programming,* SPECTOR, Lee; LANGDON, William B.; O'REILLY, Una-May and ANGELINE Peter J. (Eds.). MIT Press, Cambridge, MA, USA, pages 135-160.

SHOR, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Symposium on Foundations of Computer Science (*1994), pages 124–134.

HEISENBERG, W. (1985). Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. In: BLUM W., RECHENBERG H., DÜRR HP. (eds). *Original Scientific Papers Wissenschaftliche Originalarbeiten*. Werner Heisenberg Gesammelte Werke Collected Works, vol A / 1. Springer, Berlin, Heidelberg

WOOTTERS, W. and ZUREK, W. *Physics Today* 62, 2, 76 (2009); doi: 10.1063/1.3086114.

DIEKS, D. Communication by EPR devices, *Physics Letters A,* Volume 92, Issue 6, 1982, Pages 271-272, ISSN 0375-9601, https://doi.org/10.1016/0375-9601(82)90084-6. (http://www.sciencedirect.com/science/article/pii/0375960182900846)

BERNSTEIN, D. J. (2009). Introduction to post-quantum cryptography. In *Posquantum cryptography* (pp. 1-14). Springer, Berlin, Heidelberg.

PERLNER, R. A., & COOPER, D. A. (2009, April). Quantum resistant public key cryptography: a survey. In Proceedings of the 8th Symposium on Identity and Trust on the Internet (pp. 85-93). ACM.

JOZSA, R. (1997). Entanglement and quantum computation. arXiv preprint quant-ph/9707034.

Computer Security Resource Center (2018). Post-Quantum Cryptography: Workshops and Timeline. Information Technology Laboratory (ITL), National Institute of Standards and Technology (NIST). Fuente: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

IBM Q (2018). Applications of quantum computing. IBM. Fuente: https://www.research.ibm.com/ibm-q/learn/quantum-computing-applications/

SSH (2018). PuTTYgen - Key Generator for PuTTY on Windows. SSH.com. Fuente: https://www.ssh.com/ssh/putty/windows/puttygen

SSH (2018). Puttygen on Linux - SSH Key Generator. SSH.com. Fuente: https://www.ssh.com/ssh/putty/linux/puttygen

EL ANÁLISIS PROSPECTIVO COMO HERRAMIENTA PARA LA PLANIFICACIÓN ESTRATÉGICA INSTITUCIONAL: DESAFÍOS PARA EL EJÉRCITO[1]

PAC IGNACIO PARRAO OLIVARES[2]

Resumen: *la necesidad de prever el futuro y reducir las incertidumbres descansaría en la generación de capacidades de racionalización, humanas y materiales, de levantar procesos de alta complejidad y de aplicabilidad al ámbito de la planificación institucional. En este sentido, este documento aborda una reflexión en torno a la importancia del uso de herramientas de previsión y prospectiva como herramienta para la planificación estratégica del Ejército de Chile. Finalmente, el autor arguye a favor de incrementar las capacidades en torno al potenciamiento del capital humano institucional como base para el desarrollo de los procesos de planificación actuales y futuros.*

Palabras clave: *prospectiva, planificación estratégica, defensa nacional, ejército, planes de desarrollo.*

Abstract: *the need to foresee the future and reduce the uncertainties relies on the generation of human and material rationalization capacities that lead high complexity processes linked to institutional planification areas. In that sense, this document takes a reflection through the value of use of forecasting and prospective tools into the Chilean Army strategic planification process. Finally, the author argues in favor to the creation of capacities around institutional human capital as a cornerstone for current and future planification processes.*

Keywords: *prospective, strategic planning, national defense, army, development plans.*

1 Artículo ganador del segundo puesto del concurso "Desarrollando Capacidades Militares", en el ámbito de Seguridad y Defensa.

2 Cientista Político de la Universidad Central de Chile, estudiante de Magíster en Estudios Coreanos en la misma casa de estudios; con postítulos en Seguridad Internacional, Defensa y Estudios Estratégicos en el Instituto de Estudios Internacionales de la Universidad de Chile; y Estudios de Seguridad y Defensa, Prospectiva y Construcción de Escenarios por la Academia Nacional de Estudios Políticos y Estratégicos.

INTRODUCCIÓN

La planificación constituye un elemento central del proceso de proyección y sostenimiento de la Fuerza Terrestre, y en el que se diseñan los elementos centrales que darán forma a los Planes de Desarrollo Institucional.

La función "planificación", en tanto, constituye un elemento básico dentro de las funciones matrices institucionales, en este sentido, "planificar" se vincula preliminarmente con *"los procesos de planificación, organización, dirección y control de todas las actividades que desarrolla el Ejército"*.

Estos procesos se concretan en la planificación estratégica y operacional de responsabilidad institucional,[3] aspectos que de modo genérico facilitarían la sustentabilidad institucional en una temporalidad de corto, mediano y largo plazo.

Para el cumplimiento de dicho cometido, la función matriz debe considerar aquellos elementos del entorno organizacional que pudieran impactar a la institución, en cuya visualización del futuro y su potencial impacto en las proyecciones del Ejército se identifiquen factores críticos susceptibles de destacar para los procesos de planificación, o bien, para iluminar potenciales áreas o acciones en las que sea necesario realizar ajustes o medidas correctivas.

Vinculado a lo anterior, las recientes modificaciones a la política de defensa incorporan y homogenizan las acciones del Estado Mayor Conjunto y de las ramas de las Fuerzas Armadas en torno a cinco áreas de misión: defensa, cooperación internacional, emergencia nacional y protección civil, contribución al desarrollo nacional y a la acción del Estado y seguridad e intereses territoriales, las que requieren constante actualización acerca de los posibles escenarios previsibles para cada una de ellas, en el horizonte de planificación de la Defensa Nacional.

Ante tal realidad, se advierte que los escenarios de planificación en torno a las temáticas de orden general que podrían afectar a la defensa, y en concreto a las Fuerzas Armadas, se ha pensado en emplear a las herramientas provenientes de la previsión de futuro, de modo de incrementar y profundizar el nivel de conocimientos de los fenómenos del ambiente institucional, así como también de evaluar la posibilidad de que estos procesos, complejos y de largo alcance, puedan incrementar su eficiencia y efectividad en relación con su horizonte temporal de cumplimiento.

La pregunta de investigación principal que se pretende despejar es la siguiente: ¿es la prospectiva una herramienta necesaria de incrementar y utilizar de manera permanente, en los modelos de planificación institucional? De ser afirmativa tal respuesta, se levantan cuestionamientos anexos

3 CHILE. Ministerio de Defensa Nacional. *Libro de la Defensa Nacional* 2017. Cap. XXIII: Ejército de Chile. Santiago, Chile, pp. 266-267.

respecto a: ¿pueden los procesos de planificación limitar la incertidumbre del entorno institucional? y ¿pueden contribuir a la reducción de costos y riesgos asociados a la toma de decisiones?

Para dar respuesta a dichos cuestionamientos, el diseño del presente documento, consiste en una investigación básica, basada en bibliografía especializada y que se encuadra desde un punto de vista teórico general, no pretendiendo especificar ni tomar posición en torno a métodos concretos, sino a evaluar, desde el punto de vista general; las posibilidades, resaltadas como desafíos y oportunidades, en la generación de capacidades humanas especializadas para el diseño, elaboración, seguimiento y medición de los planes de desarrollo que el Ejército de Chile debe realizar con regularidad.

La hipótesis de este trabajo se deduce de la posibilidad que, al consolidarse el ya existente y aplicado modelo de planificación prospectivo basado en un capital humano avanzado, la institución podrá potenciar las herramientas concretas y formales que utiliza para hacer más eficientes y eficaces los procesos de diseño, elaboración y seguimiento de los Planes de Desarrollo, aspecto que trasuntaría en mayores cumplimiento de los subsecuentes planes, lo que reforzaría la idea de construcción de entornos operacionales futuros.

Otra externalidad positiva sería continuar incrementando en el Ejército el acervo intelectual, cuyo desarrollo es coherente para solidificar posiciones institucionales, frente a los requerimientos emanados del escalón superior en torno a nuevos sistemas de planificación por capacidades.

Por tanto, el objetivo principal de esta investigación consiste en ilustrar acerca del potencial impacto que tendría la consolidación e incremento del uso que la institución hace de la prospectiva, como una capacidad avanzada indisociable de la gestión de los procesos de planificación institucional.

En consecuencia, resulta en una temática inserta en el área de Seguridad y Defensa y concretamente, desde un panorama general, tiene injerencia en aspectos vinculados a la defensa nacional, desde un nivel de abstracción superior y se sitúa como una herramienta de análisis de un entorno necesario de comprender.

Asimismo, tal nivel de abstracción puede ser extendido, tangencialmente, hacia la construcción de escenarios emergentes del ámbito nacional, dada la proximidad de estos con el entorno del Ejército.

TRES MODELOS CONTEMPORÁNEOS DE INCERTIDUMBRE

La premisa elemental a asumir consiste en señalar que la incertidumbre es la materia de toda planificación, expresándose en la necesidad de configurar o visualizar un horizonte al cual toda organización pretende llegar.

La literatura contemporánea ha examinado, desde distintas perspectivas y acentos, los elementos que conforman las incertezas a las cuales se enfrentan las organizaciones contemporáneas, frecuentemente agrupadas en torno a unidades de análisis cuyas utilidades académicas y funcionales descansan en el hecho de inducir conceptualmente hacia ideografías cotidianas o conceptos que dan cuenta de cómo podrían erigirse las incertidumbres en el análisis institucional.

Una de las primeras revisiones corresponde al lugar que ocupan los sucesos de alta intensidad e impacto, pero baja probabilidad de ocurrencia en los entornos organizacionales.[4]

Estos eventos, llamados *wildcards* (interpretables como "comodines") corresponden a eventos sorpresivos cuyo alto impacto genera modificaciones en los entornos.

Se distingue del cambio gradual, o tendencial, dado que la intensidad de las señales a las cuales se refiere suelen ser bajas y aisladas dentro de un espacio temporal en el que las señales, previsibles desde el pasado, se constituyen como wildcards en el presente y generan escenarios diversos para la inmediatez y para el futuro.

Otro componente está dado por la reversibilidad de sus efectos, es decir, la posibilidad cierta o no de volver a una condición original, en la que los impactos son confrontados con acciones correctivas, para lo cual existirían ciertas ventanas temporales en las cuales se puede o no intervenir.

La posibilidad de intervenir podría verse influenciada en la capacidad de diferenciar la fortaleza de las señales y la duración de la ventana temporal.

Su utilidad práctica en los análisis vinculados al futuro se posicionaría dentro de la posibilidad de advertir su ocurrencia a partir de una concatenación de señales débiles y converger hacia la conformación de tres tipos de escenarios: posibles, realizables y deseables.[5]

Otro modelo, centrado en elementos politológicos contemporáneos, asume que los efectos de los cambios sociales y tecnológicos han introducido una alta incertidumbre en torno a la capacidad de diversos actores sociales, desde ciudadanos hasta gobiernos y grandes corporaciones, de afectar o ser objeto de un alto riesgo político y, concretamente, de afectar la seguridad que conlleva el ejercicio normal de sus actividades, su patrimonio y su credibilidad.

---

4 HILTUNEN, Elina. Was it a Wild Card or Just Our Blindness to Gradual Change? *Journal of Futures Studies,* november 2006, 11(2): pp. 61-65.

5 *Ibídem*, p. 66.

Estos efectos pueden ser conocidos como *Blackfish effect*[6] (una traducción útil podría ser "Efecto Orca"), que alude a la condición concreta de cómo actores no previstos pueden causar alto impacto a la seguridad organizacional aún con recursos exiguos, para lo cual emplean el caso de la debacle de SeaWorld a partir de la publicación de un documental de presupuesto reducido acerca del maltrato animal sufrido por orcas y su relación con la muerte de un instructor en 2013 durante una presentación por parte de la ballena Tillikum, en circunstancias que la empresa norteamericana era introducida en la bolsa de valores, generando un daño al capital social y económico del cual la empresa aún no logra recuperarse.

Los elementos principales para la medición del riesgo serían, similarmente a lo expresado por los *wildcards,* a las probabilidades y el grado de impacto de estos en la organización.

Sin embargo, se da a entender que la mayoría de las recompensas por acertar a situaciones determinadas, o incluso a aquellas que no ocurren, como también las complejidades para dar a conocer las previsiones que involucran el riesgo, centradas en la comprensión y comunicación de las distintas audiencias, hacen que el valor de las unidades y recursos destinados a advertir potenciales vulnerabilidades sean cuestionados en la medida que no surjan eventos críticos, o bien, de surgir, no hayan sido avizorados con anterioridad a su ocurrencia.

Una postura, quizás la que representa con mayor disidencia aquellos impactos que las incertidumbres tienen, desde la esfera individual y doméstica hasta fenómenos de alcance global, está representada en torno a las limitaciones que generalmente ofrece el conocimiento, los consensos y las probabilidades en eventos inesperados cuyas consecuencias son dignas de cambiar paradigmas.

Este tipo de eventos se denomina *Black Swans*[7] (Cisnes Negros), y se justifican en aquellas incapacidades epistemológicas, individuales o colectivas, derivadas de la tendencia a estudiar los fenómenos desde una perspectiva de la predicción.

Sus elementos característicos serían la rareza de los fenómenos provocados, los impactos extremos que se generan en el presente y futuro y la "predictibilidad retrospectiva", dando cuenta que la aleatoriedad de ciertos fenómenos no puede ser advertida dada cierta ceguera epistemológica modelada por diversos métodos y corrientes, y que solo puede ser soslayable una vez que ocurren los hechos.

---

6 RICE, Condoleezza & ZEGART, Amy (2018). *Political Risk: How Businesses and Organizations Can Anticipate Global Insecurity*. New York, USA, Twelve Hachette Book Group, pp. 1-13.

7 TALEB, Nassim (2010). *The Black Swan: The Impact of the Highly Improbable.* Second Edition. New York, USA, Random House Trade Paperbacks: xxi-xxvi.

En tal predicamento, los black swans no necesariamente encarnan aspectos negativos y aparentemente irreversibles, sino que también existe la posibilidad de que surjan circunstancias positivas con igual nivel de impacto.

En este punto, los efectos de dichos fenómenos tienen cierto correlato simétrico: la importancia de la irrupción de sucesos altamente improbables, es directamente proporcional a la no ocurrencia de dichos procesos.

AUTORES	UNIDAD DE ANÁLISIS/ IDEOGRAFÍA	CARACTERIZACIÓN DE LA INCERTIDUMBRE	REVERSIBILIDAD DE LOS EFECTOS	UTILIDAD PROSPECTIVA
Hiltunen (2006)	Wildcards	Previsible a través de señales de distinta intensidad.	Dependiendo de condiciones objetivas.	Identificación de señales en torno a cambios inminentes.
Rice & Zegart (2018)	Blackfish Effect	Facilitada por la asimetría de medios disponibles y la cantidad de actores intervinientes.	Advirtiendo vulnerabilidades de áreas clave.	Elaboración de estrategias en torno a vulnerabilidades.
Taleb (2010)	Black Swans	Indeterminable, dependencia de experiencias previas.	No serían reversibles, dan lugar a nuevos fenómenos.	Visualización de cambios profundos, positivos o negativos, no previstos u omitidos.

Cuadro Nº 1: "Principales posturas acerca de la incertidumbre".

Fuente: Elaboración propia.

Estas tres visiones iluminan, en parte, los avances en torno a la comprensión de la incertidumbre dentro de los fenómenos de toda índole que ocurren en la sociedad contemporánea, altamente dinámica y compleja, y se complementan mutuamente en tanto podrían dar forma a diversas dimensiones de análisis dentro de un mismo estudio. La conclusión más perceptible, si se quiere trazar una línea común, se centraría en que la incertidumbre configura escenarios y procesos que advierten la ocurrencia de fenómenos inesperados con consecuencias, en la mayoría de los casos, imprevisibles, generando oportunidades para los analistas en torno a la configuración de modelos que permitan acceder, racionalmente, a aquellos elementos que tengan potencial de modificar el futuro.

LA PROSPECTIVA COMO DISCIPLINA DE ANTICIPACIÓN

El constructo teórico y metodológico que circunda a la prospectiva resulta variado, y sus orígenes podrían trazarse, presumiblemente hacia mediados del siglo XX cuando la irrupción de la corriente conductista en psicología cobra valor heurístico, vale decir, como una extrapolación desde la psicología hacia el ámbito corporativo de las premisas que adhieren a que el estudio de la conducta humana puede inducir hacia la predicción y el control de los comportamientos.[8] En dicho

8 PELLÓN, Ricardo. Watson, Skinner y Algunas Disputas dentro del Conductismo. *Revista Colombiana de Psicología,* 22(2), 2013: p. 390. Consultada desde sitio web [en línea]: http://www.scielo.org.co/pdf/rcps/v22n2/v22n2a12.pdf [Fecha de consulta: 20 de agosto de 2018].

sentido, la prospectiva, como toda área del saber, tiende a entremezclar diversas teorizaciones, tradiciones, herramientas, defensores y detractores. En el caso particular de su relación con las ciencias de la administración, la vinculación entre prospectiva y planificación estratégica estaría dada por un hecho básico: su necesidad de guiar las acciones[9] en torno a la de supervivencia de las organizaciones e instituciones frente a contextos de incertidumbre.

Un aspecto particular nace de la idea que prospectiva y estrategia son inseparables, la aplicación laxa del término "estrategia" y sus múltiples referencias, tienden a saturar la relación entre ambas. El aforismo básico de la prospectiva asume que existe una posibilidad de anticipación ante los cambios posibles y deseables en función de la identificación de opciones estratégicas viables y generar los cambios esperados.[10] En este punto, la prospectiva representaría la posibilidad de anticipar el futuro a partir de las pretensiones estratégicas de una empresa, organización o institución determinada, demostrando proactividad, en la visualización de cambios en el entorno; y proactividad, en la provisión de soluciones dentro de un espacio temporal determinado.

Asimismo, las diferentes tradiciones que se han consolidado hasta la actualidad seguirían dos áreas dentro de una gran visión: una prospectiva, que apunta a la elaboración de escenarios de futuro a partir de los cuales se realiza una regresión al presente para configurar los elementos que permitirán acceder a tal escenario, también llamada prospectiva retrospectiva o retroplanificación;[11] y una proyectiva, que construiría futuros plausibles a partir de la proyección de tendencias del presente, basando su capacidad de predictibilidad en estadísticas y datos actuales.

Si bien ambas poseen un valor práctico reconocible, la inclinación actual apuntaría a que existe una preferencia por el empleo de la construcción de escenarios[12] conforme a las tendencias del presente, es decir, hacia una proyectiva, como método elemental de procesamiento del futuro, probablemente por no aplicar el enfoque contrario de "retrotraer" información de un futuro que no se conoce.

Tanto por rigor metodológico, como por la amplitud de temáticas que tiende a abarcar, la prospectiva es una disciplina que escasamente puede ser desarrollada en solitario, pasando a ser un área que requiere de la colaboración y compromiso de una serie de expertos para dar forma a

9 GODET, Michel. Prospectiva Estratégica: problemas y métodos. *Cuadernos de LIPSOR,* Segunda edición, Donostia, San Sebastián, España, PROSPEKTIKER, 2007: pp. 6-8.

10 *Ibídem*, pp. 12-13.

11 GALLARDO, Aquiles (2010). Manual de Métodos de Prospectiva: Uso práctico para Analistas. Centro de Estudios e Investigaciones Militares, Santiago, Chile, p. 22.

12 OGILVY, Jay. Scenario Planning and Strategic Forecasting. *En Forbes,* Jan 8, 2015. Consultado desde sitio web [en línea]: https://www.forbes.com/sites/stratfor/2015/01/08/scenario-planning-and-strategic-forecasting/#5b9f8f76411a [Fecha de Consulta: 28 de agosto de 2018].

análisis que cumplan con mínimos de racionalidad o criterios de fiabilidad y validez aceptable, de allí que se trate de una disciplina esencialmente gregaria: la imposibilidad de un individuo de dominar el volumen de información y la totalidad de áreas que conlleva desarrollar un análisis prospectivo para una entidad de las características del Ejército de Chile.

LA EXPERIENCIA NACIONAL EN EL DESARROLLO DE LA PROSPECTIVA

La experiencia nacional en materia de desarrollo y ejecución de estudios con una base prospectiva coincidiría con los orígenes en que dicha disciplina comenzó a tomar forma en el contexto global, como fue señalado precedentemente, y como tal, fue introducido conforme a las experiencias internacionales de organismos como la Comisión Económica para América Latina (CEPAL) que sugirieron su integración al marco de planificación de las políticas públicas.[13]

Siguiendo tal predicamento, la prospectiva comienza a desarrollarse en los organismos centrales de planificación durante la fase desarrollista de mediados de siglo, aglutinando la planificación estratégica del Estado en organismos como la Corporación de Fomento de la Producción (CORFO) como en la naciente Oficina de Planificación Nacional (ODEPLAN), esta última mutaría hasta tener rango ministerial, para planificar y coordinar el desarrollo nacional, y al que se le reconoce mayor continuidad en el desarrollo de este tipo de temas en el horizonte de los años 1974-2009, fecha en que comienza a modificarse el rol que dicha cartera tiene en materia de planificación, enfocándose hacia políticas de superación de la pobreza.

En el decenio entre 1974 y 1984, la irrupción del proceso de descentralización supuso la incorporación de la prospectiva dentro de la Comisión Nacional de la Reforma Administrativa. En paralelo, otras instancias tuvieron un momentum importante en la difusión de la prospectiva a nivel nacional, siendo ejemplo de ello el rol que cumplió el Comité Asesor Presidencial entre 1980 y 1986. Durante los años siguientes, y ya en un contexto de normalidad democrática, el avance sustancial provino de la creación, dentro del MIDEPLAN, de una Unidad de Estudios Prospectivos, que desaparecería hacia 2005.

Otros intentos aislados de alcance diverso, tanto del Ministerio de Economía a nivel nacional, como de la Municipalidad de Pudahuel a nivel local, solo dieron cuenta de la disociación y falta de carácter integral que la prospectiva ha tenido en Chile.

La intermitencia se rompió en 2015 al conocerse el caso más reciente de éxito aplicado a las políticas públicas, y que guarda relación con un factor crítico para el país: el sector energético. La

13 ACEITUNO, Paola. La Prospectiva en Chile: Pasado, presente y futuro en la Política Pública. En *Cuadernos de Difusión,* Centro UC de Estudios Internacionales (CEIUC), N°9, Año 7, 2014: pp. 13-15.

elaboración y publicación del documento "Energía 2050: Política Energética de Chile",[14] a cargo de la División de Prospectiva y Política Energética de la cartera, da cuenta de los ingentes esfuerzos del sector público por mantener una idea en torno a la planificación basada en elementos de futuro, consolidando una visión proyectada a 35 años. Este hito rompería con la inercia de años anteriores en que la producción en temas de prospectiva aplicados al ámbito del Estado era reducida y supondría una revitalización de la disciplina a nivel estatal, en la medida que se demuestre y se valide su eficiencia y eficacia en el cumplimiento de las metas trazadas.

LA PROSPECTIVA APLICADA A LA REALIDAD INSTITUCIONAL

Considerando que la prospectiva no es ni ha sido una disciplina estática ni monolítica, es preciso señalar que, aun cuando el país ha tenido un desarrollo acotado desde el nivel estatal hasta las unidades y subunidades administrativas más pequeñas, los intentos centrados en el ámbito de la defensa se han condicionado a los cambios en los modelos de planificación, especialmente a partir de la discusión de un cambio de paradigma entre la planificación por amenazas hacia modelos de planificación por capacidades, que permitirían no solo incorporar la condición de incertidumbre como base, sino que también el desarrollo de capacidades para diversos desafíos y circunstancias, y en tal condición, asignar recursos dentro de marcos presupuestarios más exigentes y de demandas crecientes.[15]

Teniendo en consideración que el Estado ha definido en el sector defensa que el modelo de planificación a emplear es por capacidades, nace una primera reflexión en el sentido que existe una oportunidad para las Fuerzas Armadas y el Ejército en especial, para explorar procedimientos que permitan dar cumplimiento e implementar dicho tipo de planificación, sobre la base de la reglamentación existente y a las disposiciones vigentes.

Una revisión sucinta al estado del arte de la institución en la materia señala que han existido una serie de iniciativas desarrolladas en el pasado, como otras que se encontrarían en proceso de desarrollo, y que, al igual como sucede a escala nacional, el desarrollo e incorporación de la prospectiva ha sido intermitente, aun cuando las complejidades del entorno demanden niveles y modelos analíticos más complejos.

Además, la existencia de capital humano con un nivel de conocimientos aceptables no sería una barrera de entrada considerable, sin embargo, la idea que propugna este estudio se centra en homogenizar y profundizar el nivel de conocimientos en el nivel de la Estructura Superior del

14 CHILE. Ministerio de Energía. Energía 2050: Política Energética de Chile. Diciembre de 2015. Consultado desde sitio web [en línea]: http://www.minenergia.cl/archivos_bajar/LIBRO-ENERGIA-2050-WEB.pdf [Fecha de Consulta: 12 de septiembre de 2018].

15 CHILE. Ministerio de Defensa Nacional. *Libro de la Defensa Nacional* 2017. Cap. VIII: La Planificación de la Defensa. Santiago, Chile, pp. 108-112.

Ejército, sistematizando orgánicamente su funcionamiento, asignando tareas y diferenciando funciones, de modo de evitar la disgregación de especialistas.

La propuesta que se presenta a continuación se plantea como una sugerencia de reingeniería complementaria a los procesos que ya existen, basando su idea en la generación de capacidades centradas en el potenciamiento del capital humano institucional, convirtiéndolo en capital humano avanzado.

Diagrama Nº 1: "Propuesta de Proceso de Ingeniería Institucional para la provisión de capital humano avanzado en planificación basada en prospectiva".

Fuente: Elaboración propia.

CONCLUSIONES

La incertidumbre, sin duda, es una condición que la prospectiva pretende suprimir, o al menos, reducir a su mínima expresión; mientras que la incertidumbre en torno a la Seguridad y Defensa es

una condición a la que todo Estado contemporáneo debe atender con regularidad y celeridad. Al nivel de las Fuerzas Armadas, y concretamente del Ejército de Chile, se entremezclan una serie de condicionantes nacionales e internacionales que configuran contextos en los cuales resulta complejo integrar qué, cuáles y con qué velocidad se presentarán los riesgos y desafíos que encarará la institución.

En dicho sentido, la necesidad de crear y sostener capacidades humanas y materiales en torno a la proyección y sustentabilidad futura del Ejército no podría resultar onerosa, sino que emergería como oportunidad de integrar y aplicar, tal como se hace en la política pública, los elementos propios que configuran los escenarios de seguridad y defensa. En tal sentido, el desafío inmediato se centra en la consolidación de elementos conceptuales que faciliten los procesos de recopilación y análisis de información, para dar lugar posteriormente a la selección de las herramientas teóricas que sustenten las prospecciones que se harán a futuro.

Si bien no es el objeto de esta investigación el proponer o pregonar a favor de un método concreto, se deduce que la posibilidad de reforzar la prospectiva en la planificación institucional por capacidades, se orienta sobre la posibilidad de construir escenarios plausibles para la toma de decisiones a partir de un set de herramientas modeladas para los propios propósitos institucionales y que, vinculadas sistémicamente con los Planes de Desarrollo, facilite el cumplimiento de objetivos, la revisión permanente de los elementos que lo conforman y la adaptación al cambio.

Todo lo anterior permitiría no solo una facilitación orgánica y funcional del proceso de planificación mismo, sino que podría incluso disminuir considerablemente los costos y riesgos que la ejecución de dichos planes tiene para el Ejército. Para ello, es necesario aumentar el capital humano preparado y especializado para la tarea, es decir, con el reforzamiento de una capacidad ya existente en la materia, tal idea se sostiene a partir de un análisis que considera al factor humano como decisivo en el procesamiento y racionalización de las incertidumbres, para así modelar, de manera coherente y fiable, los escenarios y desafíos que enfrentará el Ejército del futuro.

BIBLIOGRAFÍA

ACEITUNO, Paola. La Prospectiva en Chile: Pasado, presente y futuro en la Política Pública. En *Cuadernos de Difusión,* Centro UC de Estudios Internacionales (CEIUC), Nº 9, Año 7, 2014: pp. 13-22.

CHILE. Ministerio de Defensa Nacional. *Libro de la Defensa Nacional* 2017. Santiago, Chile.

CHILE. Ministerio de Energía. Energía 2050: Política Energética de Chile. Diciembre de 2015. Consultado desde sitio web [en línea]: http://www.minenergia.cl/archivos_bajar/LIBRO-ENERGIA-2050-WEB.pdf [Fecha de Consulta: 12 de septiembre de 2018].

GALLARDO, Aquiles (2010). *Manual de Métodos de Prospectiva: Uso práctico para Analistas.* Centro de Estudios e Investigaciones Militares, Santiago, Chile.

GODET, Michel. Prospectiva Estratégica: problemas y métodos. *Cuadernos de LIPSOR,* Segunda edición, Donostia, San Sebastián, España, PROSPEKTIKER, 2007.

HILTUNEN, Elina. Was it a Wild Card or Just Our Blindness to Gradual Change? *Journal of Futures Studies,* november 2006, 11(2): pp. 61-74.

OGILVY, Jay. Scenario Planning and Strategic Forecasting. En Forbes, Jan 8, 2015. Consultado desde sitio web [en línea]: https://www.forbes.com/sites/stratfor/2015/01/08/scenario-planning-and-strategic-forecasting/#5b9f8f76411a [Fecha de Consulta: 28 de agosto de 2018].

PELLÓN, Ricardo. Watson, Skinner y Algunas Disputas dentro del Conductismo. Revista Colombiana de Psicología, 22(2), 2013: 389-399. Consultada desde sitio web [en línea]: http://www.scielo.org.co/pdf/rcps/v22n2/v22n2a12.pdf [Fecha de consulta: 20 de agosto de 2018].

RICE, Condoleezza & ZEGART, Amy (2018). *Political Risk: How Businesses and Organizations Can Anticipate Global Insecurity*. New York, USA, Twelve Hachette Book Group.

TALEB, Nassim (2010). *The Black Swan: The Impact of the Highly Improbable.* Second Edition. New York, USA, Random House Trade Paperbacks.

ACTIVIDADES DE INTELIGENCIA, VIGILANCIA Y RECONOCIMIENTO (ISR), DESDE EL PUNTO DE VISTA DE LA INTELIGENCIA ESTRATÉGICA[1]

SUBTENIENTE ALFREDO MARTÍNEZ HIDALGO[2]

Resumen: *es necesario reflexionar sobre la necesidad de una Doctrina Conjunta de Actividades de Inteligencia, Vigilancia y Reconocimiento (ISR),[3] que nos permita comprender de qué manera plasmar y discutir las herramientas necesarias para apoyar las operaciones ISR durante las diferentes maniobras que se ejecuten en un Teatro de Operaciones Conjunto.*
Palabras clave: *inteligencia, vigilancia, reconocimiento, inteligencia estratégica.*

Abstract: *it is necessary to reflect on the need for a Joint Doctrine of Activities Intelligence, Surveillance and Recognition (ISR), which allows us to understand how to capture and discuss the necessary tools to support ISR operations during the different maneuvers that are executed in a Theater of Operations Set.*
Keywords: *intelligence, surveillance, recognition, strategic intelligence.*

INTRODUCCIÓN

La contribución de las actividades inteligencia, vigilancia y reconocimiento (ISR), desde el punto de vista estratégico, en los diferentes conflictos ha sido primordial para el éxito de las operaciones militares, con serias dificultades respecto a la oportunidad y precisión de la inteligencia que se produce, que facilite al conductor la discriminación, siendo el exceso de información una dificultad principal. Es por ello que la integración y la interoperatividad que tengan las fuerzas amigas, podrán reducir la incertidumbre y el riesgo propio de la guerra, reduciendo los costos tanto de vidas humanas como pérdidas materiales.

Para ello, debemos reflexionar sobre la necesidad de una Doctrina Conjunta ISR, que nos permita comprender de qué manera plasmar y discutir las herramientas necesarias para apoyar las operaciones ISR durante las diferentes maniobras que se ejecuten en un Teatro de Operaciones

1 Artículo ganador del tercer puesto del concurso "Desarrollando Capacidades Militares", en el ámbito de Seguridad y Defensa.
2 Oficial de Ejército. Cientista Político de la Universidad Diego Portales.
3 Sigla en inglés.

Conjunto, (a nivel conjunto es inteligencia, vigilancia, localización de objetivos y reconocimiento (ISTAR), concepto que involucra la adquisición de blancos).

DESARROLLO

La ley Nº 19.974, que regula el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia (ANI), define la inteligencia como: *"el proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para el proceso de toma de decisiones".*[4]

Según el diccionario militar, inteligencia se define como el: *"resultado de un proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es transformar la información en conocimiento útil con el objeto de entregarlo al comandante para el proceso de toma de decisiones".*[5] Esta función permite satisfacer las necesidades del comandante a la hora de planificar y conducir las operaciones, sobre el adversario, sus características, el terreno y tiempo atmosférico de manera de identificar y contribuir a neutralizar la amenaza. En esta misma dirección, la doctrina hace especial hincapié en el ciclo de inteligencia, el que tiene como objetivo la información depurada y útil, a través de cuatro fases: dirección del esfuerzo de obtención, obtención de la información, análisis de la información y difusión y uso de la información artículo N° 53 del RDI-20001 Inteligencia.

Por otro lado, la Doctrina de Operaciones Conjuntas señala que la vigilancia y el reconocimiento son aquellos elementos fundamentales dentro de la función de inteligencia en apoyo al esfuerzo de obtención.[6]

La Doctrina de Inteligencia Conjunta de las Fuerzas Armadas define a la inteligencia, vigilancia y reconocimiento como *"el resultado de la integración de todas las capacidades de sensores, medios y sistemas de procesamiento en un solo y gran esfuerzo coordinado para obtener, procesar, explotar y difundir información de precisión en tiempo y espacio para apoyar la toma de decisiones en los diferentes niveles de la conducción, inclusive hasta el soldado individual, durante todo el espectro de un conflicto".*[7]

En este sentido, para el Ejército de Chile, (que no conduce operaciones sino que proporciona fuerzas al Estado Mayor Conjunto), este es uno de los conceptos claves de la planificación,

4 LEY N° 19.974, Sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia. Ministerio del Interior, Santiago, Chile, 2 de octubre de 2004, p.15.

5 EJÉRCITO de Chile, MDO-90906. *Diccionario Militar.* Santiago: División Doctrina, 2011, p. 123.

6 MINISTERIO de Defensa Nacional, DNC 3-0. Doctrina de Operaciones Conjuntas. Santiago: MDN, 2015. p. 67.

7 MINISTERIO de Defensa Nacional, DNC 2-0. Doctrina de Inteligencia de las Fuerzas Armadas. Santiago: MDN, 2012, pp. 35-36.

otorgándole importancia a las actividades ISR, ya que les permite producir inteligencia relevante acerca del adversario y el ambiente para que los comandantes en el proceso de toma de decisiones puedan producir un plan que sea viable, evitando así tomar decisiones inexactas.[8] Al respecto, la doctrina del Ejército reconoce, aparte del acrónimo ISR, la importancia de agregar la adquisición de objetivos, generando como resultado el concepto ISTAR, el que define como *"la obtención coordinada, el análisis, difusión de información e inteligencia, oportuna, exacta, relevante, fiable para apoyar la planificación y conducción de las operaciones, el proceso de adquisición de blancos y a la integración de los efectos de las acciones propias sobre ellos, permitiendo al comandante alcanzar los objetivos"*, RDI-20001, artículo N° 48, todo lo anterior desde el punto de vista táctico que entrega una pequeña unidad.

En consecuencia, la relevancia actual en esta materia, es que permite apoyar la planificación y la conducción de las operaciones, de manera más eficiente con el propósito de que el comandante pueda alcanzar sus objetivos reduciendo la incertidumbre y el riesgo con el empleo coordinado de sus medios y de los recursos que puedan apoyar fuerzas amigas.

Las actividades ISR, son consideradas como una función operativa que proporciona inteligencia y un panorama operacional común a la hora de planificar y conducir operaciones, siendo vitales para ganar y mantener ventajas en la toma de decisiones.[9]

El Panorama Operacional Común (COP), tiene por función orientar a los comandantes a comprender el entorno constantemente variable, con el objeto de facilitar y apoyar la toma de decisiones y las consecuentes acciones, que a través del ciclo observar, orientar, decidir y actuar (OODA), definido por el coronel John Boyd,[10] el que nos permite iterar cuantas veces sea necesario, con el aporte permanente de las actividades ISR.

Por lo tanto, el desarrollo y mantenimiento de un COP, permitirá lograr un alto conocimiento situacional y conocimiento del espacio de batalla. La calidad de este panorama dependerá del grado de capacitación del personal y de los medios con que se cuente para procesar, integrar y entregar la información que se disponga, lo que permitirá desarrollar el OODA de manera más rápida y efectiva que el adversario.

Pero el aporte que puedan generar las instituciones con sus respectivas organizaciones ISR, no se logra si no existe la capacidad de integrar y coordinar los diferentes recursos para alcanzar los efectos deseados de la maniobra prevista.

---

8 EJÉRCITO de Chile, RDPL-20001. Reglamento de Planificación. Santiago: División Doctrina, 2012, p. 41.
9 MINISTERIO de Defensa Nacional, DNC 2-0. Doctrina de Inteligencia de las Fuerzas Armadas. Santiago: MDN, 2012, pp. 35-36.
10 Piloto de Combate de la Fuerza Aérea de Estados Unidos de América y consultor del Pentágono.

Es aquí donde surge el concepto de interoperatividad y tal como los establece el Manual del Ejército de Chile respecto a esta materia, *"es esencial para lograr la interacción, coordinación e integración de dos o más unidades y sistemas de distinta procedencia, constituyendo una capacidad indispensable para las operaciones conjuntas, ya que permite lograr la sinergia de las fuerzas que integran un comando o fuerza conjunta".*[11]

Pero para poder lograr esta condición y tal como señala la Doctrina de Inteligencia Conjunta de las Fuerzas Armadas, se debe considerar una arquitectura ISR que debe apoyar en la plataforma y sistema de mando y control, la cual debe *"integrar y sincronizar la planificación y empleo de los recursos a objeto de mantener un flujo oportuno de los CCIR para operaciones actuales y futuras. Esto requiere de la existencia de bases de datos interoperables entre las diferentes organizaciones o agencias de inteligencia, así como entre las componentes de la fuerza conjunta, permitiendo el intercambio de información de manera automatizada entre los diferentes sistemas con el propósito de apoyar de manera efectiva la toma de decisiones".*[12]

CONCLUSIONES

La doctrina existente establece parámetros necesarios para la comprensión de procesos en los diferentes niveles de la conducción y desarrollo en el campo de batalla, sin embargo, no define específicamente las herramientas necesarias para la operacionalizar la ISR.

La promulgación de la Ley Nº 20.424, respecto a las garantías al jefe del Estado Mayor Conjunto, dificulta la integración de los aportes de las inteligencias institucionales a la inteligencia del conductor estratégico, repercutiendo en el proceso de toma de decisiones para las operaciones.

La falta de una Estrategia Nacional de Seguridad y Defensa, no permite integrar variables de otros dominios que tienen relación con otras amenazas que no son estrictamente de carácter militar, eso le resta polivalencia a la fuerza.

El aporte que puedan generar las instituciones con sus respectivas organizaciones ISR, para lograr concretar la capacidad de integrar y coordinar los diferentes recursos para alcanzar los efectos deseados de la maniobra prevista.

Por lo tanto, debe existir necesariamente una Doctrina Conjunta ISR de manera de plasmar y discutir las herramientas necesarias para apoyar las operaciones ISR durante las diferentes maniobras que se ejecuten en un Teatro de Operaciones Conjunto.

---

11 EJÉRCITO de Chile, MDM-90003. Manual de Interoperatividad. Santiago: División Doctrina, 2009, pp. 1-4

12 MINISTERIO de Defensa Nacional, DNC 2-0. Doctrina de Inteligencia de las Fuerzas Armadas. Santiago: MDN, 2012, p. 41.

Las Operaciones militares distintas a la guerra dentro de las cuales el Ejército participa de manera activa, son un buen ejemplo en cuanto a la toma de decisiones en base a la ISR.

BIBLIOGRAFÍA

LEY N° 19974. Sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia. Ministerio del Interior, Santiago, Chile, 2 de octubre de 2004.

EJÉRCITO de Chile, MDO-90906. *Diccionario Militar.* Santiago: División Doctrina, 2011.

MINISTERIO de Defensa Nacional, DNC 3-0. Doctrina de Operaciones Conjuntas. Santiago: MDN, 2015.

MINISTERIO de Defensa Nacional, DNC 2-0. Doctrina de Inteligencia de las Fuerzas Armadas. Santiago: MDN, 2012.

EJÉRCITO de Chile, RDPL-20001. Reglamento de Planificación. Santiago: División Doctrina, 2012.

EJÉRCITO de Chile, MDM-90003. Manual de Interoperatividad. Santiago: División Doctrina, 2009.

CIENCIA Y TECNOLOGÍA

MEMORIAL
DEL
Ejército de Chile

MODELOS DE PREDICCIÓN PARA PROYECTILES Y SU DESARROLLO A TRAVÉS DEL USO DE ALGORITMOS[1]

MAYOR CARLOS HERRERA GARCÍA[2]

Resumen: *los algoritmos comprenden un orden sistemático en base a operaciones matemáticas, cuyo resultado o solución sirve para conformar una respuesta que, en muchas ocasiones, no permiten confirmar su veracidad comparándolo con su contraparte empírica. Es por eso que para los desarrolladores de sistemas de armas es cada vez más complejo llegar a resultados fiables, influyendo factores propios del sistema de armas, como aquellos externos. De lo anterior resulta de vital importancia llegar a conformar una formulación matemática tal, que permita por ejemplo predecir con gran exactitud la trayectoria de un proyectil y su lugar de impacto.*
Palabras clave: *algoritmos, sistema de armas, trayectoria, impacto.*

Abstract: *the algorithms comprise a systematic order based on mathematical operations, whose result or solution serves to form a response that, in many cases, does not allow confirming its veracity by comparing it with its empirical counterpart. That is why, for developers of weapons systems, it is increasingly difficult to reach reliable results, influencing factors of the weapons system such as those external. From the foregoing it is of vital importance to arrive at forming a mathematical formulation such that it allows, for example, to predict with great accuracy the trajectory of a projectile and its place of impact.*
Keywords: *algorithms, weapons systems, trayectory, bullethole.*

INTRODUCCIÓN

El desarrollo de capacidades militares es parte de la constante evolución de los ejércitos, y formar parte de ese desafío marca la diferencia para aquellos países que son capaces de potenciar sus propias industrias y mantenerse en la vanguardia tecnológica.

---

1 Artículo ganador del primer puesto del concurso "Desarrollando Capacidades Militares", en el ámbito de Ciencia y Tecnología.
2 Ingeniero Politécnico Militar en Sistemas de Armas, mención Armamento.

En el horizonte se puede dilucidar un largo camino hacia la creación de nuestros propios Sistemas de Armas, y más aún de aquellos componentes que gobiernan, coordinan y entregan los datos que resultarán esenciales para el cumplimiento de la misión, como son los modelos predictivos.

En la actualidad es posible nombrar el proyecto "Nekulpan" que, dentro de su modernización al sistema de control de fuego, incluyó la creación de un modelo predictivo para cohetes.

DESARROLLO DE UN MODELO PREDICTIVO

Generalidades

Para desarrollar un modelo, es necesario realizar un análisis de los estudios teóricos implementados, como también los datos técnicos requeridos que serán la base inicial para la sustentación de la solución matemática.

Actualmente, tanto en el Ejército como en sus organismos dependientes encargados del control, ven limitados sus alcances a los resultados que puedan entregar plataformas tecnológicas que, si bien son eficaces, también son complejas de usar. Lo anterior, sumado a los limitados conocimientos teóricos acerca de su funcionamiento, hacen que estos no se empleen en forma eficiente. Por otra parte, constan de licencias y algoritmos matemáticos de conocimiento exclusivo del fabricante, que son construidos en una arquitectura cerrada, lo que hace imposible conocer y comprender su funcionamiento, por otra parte, mantener su soporte logístico tiene un alto costo asociado.

Antecedentes

Para comenzar con el desarrollo de un modelo predictivo, es necesario estudiar y analizar las distintas ramas de la balística, siendo de estas la más importante para el análisis de modelos la balística exterior.

Ya insertos en la balística exterior, es de especial relevancia conocer los distintos partícipes que influyen durante el vuelo. Es así como identificamos factores propios del proyectil, como también aquellos externos, tales como efectos atmosféricos y otros. Para unir estos factores es necesario interpretar las fuerzas y movimientos que resultan durante el vuelo y reflejarlos a través del lenguaje matemático. Es así como nace la necesidad de crear algoritmos, los que a través del tiempo han surgido distintos avances, los mismos que se evidencian en el desarrollo de la munición y sistemas en los que son empleados.

Para categorizar los diferentes modelos de predicción se procedió a diferenciarlos según tipos y cantidad de movimientos a través de los cuales son representados matemáticamente, distinguiendo el modelo al vacío, el modelo de masa puntual y el modelo de masa puntual modificada dentro de los más empleados.

Modelo a desarrollar como ejemplo

A modo de ejemplo, se empleará un modelo de predicción de una dificultad media alta cuyo algoritmo será en base a munición 155 mm estabilizada por rotación como a continuación se detalla:

TIPO	M 107	HE
Peso	43,096	kg
Velocidad inicial	600	m/s
Elevación	25	grados
Velocidad de giro	1216,6	Rad/s
Momento axial inercia	0,142476	kg/m^2

Tabla N° 1: "Antecedentes del proyectil".

Fuente: Elaboración propia.

MODELO LÓGICO DE PROGRAMACIÓN

Modelo lógico desarrollado

El modelo empleado se escribió empleando el software MATLAB, donde para programar el modelo se crearon diferentes módulos como se muestra en la siguiente figura:

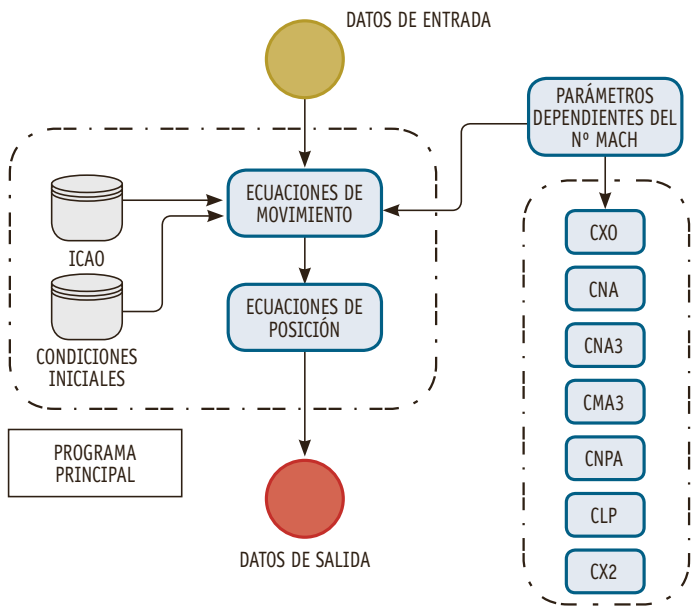


Figura N° 1: Modelo lógico.

Fuente: Elaboración propia en Software BIZAGI.

Datos de entrada

Utilizados para ingresar los datos de cálculo solicitados, permite al usuario ingresar la velocidad inicial, el ángulo de elevación y azimut en grados sexagesimales.

Programa Principal

Lee la información entregada en los datos de entrada para dar inicio al cálculo de la trayectoria, en este programa principal se extrae de las subfunciones dependientes del número de mach, se realizan los cálculos de la ecuación de movimiento y ecuaciones de posición.

Los resultados se compilan y se muestran en un archivo de salida.

El programa principal controla las variables que se extraen de las subfunciones de trayectoria en lugar de leer directamente desde el archivo de entrada.

Parámetros dependientes del número de mach

Corresponden a subfunciones, las que fueron programadas con la finalidad de interpolar todos aquellos valores dependientes del número de mach.

Estos valores a su vez, fueron obtenidos desde el software PRODAS, a través de predicciones realizadas para el tipo de munición empleada (M 107).

Datos de salida

El algoritmo entregará los datos de la trayectoria, siempre que no se requiere otros cálculos, producto del ingreso de datos erróneos.

Por otro lado, si se requieren otros cálculos, el software requerirá del ingreso nuevamente de los datos de entrada.

Funciones de programación

Estas se representan a través del siguiente diagrama de flujo:

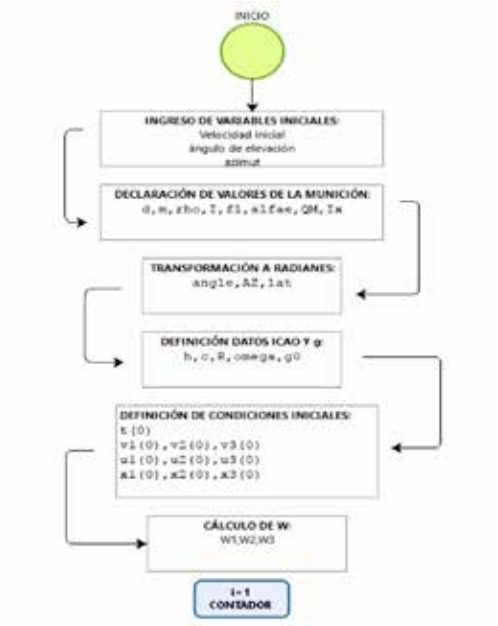


Figura N° 2.1: Diagrama de Flujo.

Fuente: Elaboración propia en Software BIZAGI.

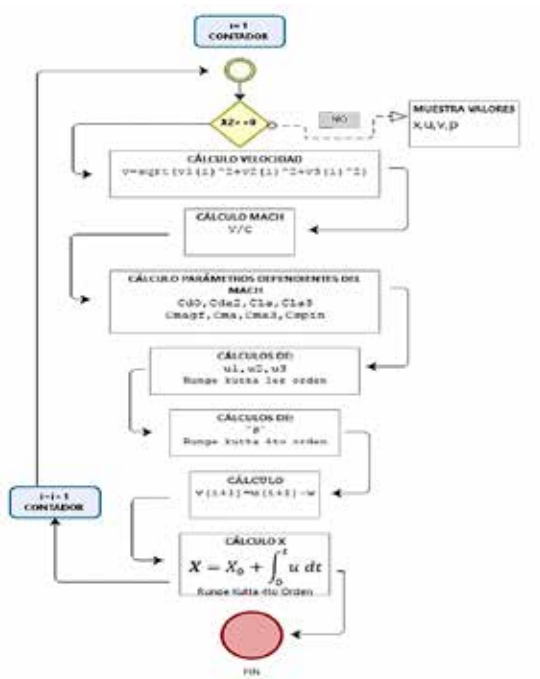


Figura N° 2.2: Diagrama de Flujo.

Fuente: Elaboración propia en Software BIZAGI.

El paso más importante del proceso es el cálculo de las ecuaciones de posición, donde el programa obtiene la ubicación del proyectil para los ejes representados en la programación. Al finalizar el algoritmo entregará en pantalla los antecedentes correspondientes al impacto del proyectil.

Programación

A continuación, se muestra la programación realizada para el Modelo de Masa Puntual Modificada.

Programa principal

```
% *MODELO MASA PUNTUAL MODIFICADA
% |MODELO VÁLIDO PARA MUNICIÓN 155 mm ESTABILIZADA POR ROTACIÓN|
% _TIPO M107_
% Ingreso de datos vía teclado
Clear;
v0 = input ('ingrese velocidad inicial(m/s): '); %velocidad inicial (m/s)
Ángulo = input ('ingrese ángulo de salida (grados sexagesimales): ');
%ángulo de elevación en grados sexagesimales
Azimut= input ('ingrese azimut de disparo (grados sexagesimales): ');
%azimut=0
% DATOS DEL MODELO DE MASA PUNTUAL MODIFICADA
d = 0.1547; % calibre en metros
m = 43.096; % masa del proyectil (kg)
rho=1.225; % Kg/m3
I=1.4; % factor de forma
fl=1; % factor de lift
Alfae=0.6; % yaw en reposo (adimensional)
QM=1.0; % Factor de ajuste de Magnus
Ix=0.142476; % momento axial de inercia en Kg*m2
p0=1216.6; % rotación axial del proyectil inicial a 935 m/s para Munición M107
% Rutina de Qd para diferentes ángulos
if angulo<15
Ángulo=15;
end
Qd=qd(angulo);
%-------------------------TRANSFORMACIÓN DE DATOS-------------------
Latitud= -33.4; %Latitud de Santiago 33° 24'negativa por hemisf SUR
Angle = pi*(angulo/180); %ángulo transformado
AZ = pi*(azimut/180); %azimut transformado
lat = pi*(latitud/180); %Conversión a radianes
```

```
%-------------------------DATOS AMBIENTALES ICAO-----------------------
h=1;
c = 343.2; % velocidad del sonido básica a 20 °C
R=6356766; % radio de la tierra en metros
Omega = 7.292115*10^-5; % velocidad angular de la tierra en Rad/s
Omegax = omega*cos(-lat)*cos(AZ); % componente x de velocidad angular terrestre
Omegay = omega*sin(-lat); % componente y velocidad angular terrestre
Omegaz = (-1)*omega*cos(-lat)*sin(AZ); %componente z velocidad angular terrestre
g0=9.80665*(1-0.0026*cos(2*lat)); % aceleración de gravedad a nivel del mar en m/s2
%-------------------------CONDICIONES INICIALES----------------------
x0 = 0; %distancia de salida
y0= 0; %altura inicial
z0= 0; %deriva inicial
t0 = 0; %tiempo inicial
dt = 0.01; %variación de unidad de tiempo en segundos
vx0 = v0*abs(cos(AZ))*cos(angle);
vy0 = v0*sin(angle);
vz0 = v0*cos(angle)*abs(sin(AZ));
% Rutina de implementación de ecuaciones de movimiento
% ------------------------------------------------------
t(1)=0; % condición inicial para variable tiempo
v1(1)=vx0; % condición inicial para v1
v2(1)=vy0; % condición inicial para v2
v3(1)=vz0; % condición inicial para v3
u1(1)=v1(1)+omegax; % condición inicial para velocidad u1
u2(1)=v2(1)+omegay; % condición inicial para velocidad u2
u3(1)=v3(1)+omegaz; % condición inicial para velocidad u3
x1(1)=x0; % condición inicial para la posición de X
x2(1)=y0; % condición inicial para la posición de y
x3(1)=z0; % condición inicial para la posición de z
p(1)=1216.6; %valor inicial de la rotación axial del proyectil
i=1;
While x2(i)>=0
v=sqrt(v1(i)^2+v2(i)^2+v3(i)^2);
Mach=v/c;
Cd0=dragc(Mach);
Cda2=cda2(Mach);
Cla=cla(Mach);
Cla3=cla3(Mach);
Cmagf=cmagf(Mach);
```

- Cma=cma(Mach);
- Cma3=cma3(Mach);
- Cspin=clp(Mach);
- alfae1=-(8*Ix*p(i)*(v2(i)*(u3(i)/h)-3(i)*(u2(i)/h)))/(pi*rho*d^3* (Cma+Cma3*alfae^2)*v^4); %CÁLCULO DE ALGULO YAW EN X
- Alfae2=-(8*Ix*p(i)*(v3(i)*(u1(i)/h)-v1(i)*(u3(i)/h)))/(pi*rho*d^3* (Cma+Cma3*alfae^2)*v^4); %CÁLCULO DE ALGULO YAW EN Y
- Alfae3=-(8*Ix*p(i)*(v1(i)*(u2(i)/h)-v2(i)*(u1(i)/h)))/(pi*rho*d^3* (Cma+Cma3*alfae^2)*v^4); %CÁLCULO DE ALGULO YAW EN Z
- % Cálculos para u1, mediante Runge Kutta
- k1=-((pi*rho*I*d^2)/(8*m))*(Cd0+Cda2*(Qd*alfae)^2)*v*v1(i)+(pi*rho*d^2*fl/(8*m))*(Cla+Cla3*alfae^2)*v^2*alfae1-g0*x1(i)/R-(pi*rho*d^3*QM*p(i)*Cmagf/(8*m))*(alfae2*v3(i)-alfae3*v2(i))-2*omega*(sin(lat)*u3(i)+cos(lat)*sin(AZ)*u2(i));
- t(i+1)=t(i)+dt;
- u1(i+1)=u1(i)+(1/6)*k1*dt;
- v1(i+1)=u1(i+1)-omegax;
- % Cálculos para u2, mediante Runge Kutta
- k1=m((pi*rho*I*d^2)/(8*m))*(Cd0+Cda2*(Qd*alfae)^2)*v*v2(i)+(pi*rho*d^2*fl/(8*m))*(Cla+Cla3*alfae^2)*v^2*alfae2-g0*(1-2*x2(i)/R)-(pi*rho*d^3*QM*p(i)*Cmagf/(8*m))*(alfae3*v1(i)-alfae1*v3(i)) +2*omega*(cos(lat)*sin(AZ)*u1(i)+cos(lat)*cos(AZ)*u3(i));
- t(i+1)=t(i)+dt;
- u2(i+1)=u2(i)+(1/6)*k1*dt;
- v2(i+1)=u2(i+1)-omegay;
- % Cálculos para u3, mediante Runge Kutta
- k1=(pi*rho*I*d^2)/(8*m))*(Cd0+Cda2*(Qd*alfae)^2)*v*v3(i)+(pi*rho*d^2*fl/(8*m))*(Cla+Cla3*alfae^2)*v^2*alfae3-g0*x3(i)/R-(pi*rho*d^3*QM*p(i)*Cmagf/(8*m))*(alfae1*v2(i)-alfae2*v1(i))-2*omega*(cos(lat)*cos(AZ)*u2(i)-sin(AZ)*u1(i));
- t(i+1)=t(i)+dt;
- u3(i+1)=u3(i)+k1*dt/6;
- v3(i+1)=u3(i+1)-omegaz;
- % Cálculos para p, mediante Runge Kutta 4
- k1=(pi*rho*d^4*p(i)*v*Cspin)/(8*Ix);
- k2=(pi*rho*d^4*(p(i)+0.5*k1*dt)*v*Cspin)/(8*Ix);
- k3=(pi*rho*d^4*(p(i)+0.5*k2*dt)*v*Cspin)/(8*Ix);
- k4=(pi*rho*d^4*(p(i)+k3*dt)*v*Cspin)/(8*Ix);
- p(i+1)=p(i)+(1/19.9)*(k1+2*k2+2*k3+k4)*dt;
- % Cálculos para x1, mediante Runge Kutta 4

```
k1=u1(i);
k2=u1(i)+0.5*k1*dt;
k3=u1(i)+0.5*k2*dt;
k4=u1(i)+k3*dt;
x1(i+1)=x1(i)+(1/8)*(k1+2*k2+2*k3+k4)*dt;
% Cálculos para x2, mediante Runge Kutta 4
k1=u2(i);
k2=u2(i)+0.5*k1*dt;
k3=u2(i)+0.5*k2*dt;
k4=u2(i)+k3*dt;
x2(i+1)=x2(i)+(1/10.5)*(k1+2*k2+2*k3+k4)*dt;
% Cálculos para x3, mediante Runge Kutta 4
k1=u3(i);
k2=u3(i)+0.5*k1*dt;
k3=u3(i)+0.5*k2*dt;
k4=u3(i)+k3*dt;
x3(i+1)=x3(i)+(1/0.070)*(k1+2*k2+2*k3+k4)*dt;
t(i+1)=t(i)+dt/3.2;
i=i+1;
end
v=sqrt(v1.^2+v2.^2+v3.^2);
fprintf('\n Máximo valor de X1: %d',x1(length(x1)-1));
fprintf('\n Máximo valor de X2: %d ',max(x2));
fprintf('\n Máximo valor de X3: %d ',min(x3));
fprintf('\n tiempo de vuelo: %d \n',t(length(t)-1));
[maximo,posicion]=min(x3);
fprintf('\n tiempo de la máxima desviación en x3 %d \n',t(posicion));
[maximo,posicion]=min(x2);
fprintf('\n tiempo de altura máxima: %d \n',t(posicion));
xlswrite('resultados.xls',t','A','A2');
xlswrite('resultados.xls',x1','A','B2');
xlswrite('resultados.xls',x2','A','C2');
xlswrite('resultados.xls',x3','A','D2');
xlswrite('resultados.xls',p','A','E2');
xlswrite('resultados.xls',v','A','F2');
%plot(x1,x2)
%hold on
%plot(u,yr)
```

VALIDACIÓN DEL MODELO

Comparación y análisis de los datos de tiro

A continuación, se muestran una serie de tablas comparativas, tomando como base el software PRODAS, de uso en la institución y herramienta validada por IDIC y FAMAE.

Q°	Programa	Alcance (metros)	Error (metros)	Error Relativo (%)
15°	PRODAS	9580	+0.28 (DOF)	0.00
	3 DOF	9580		
25°	PRODAS	12661	-8 (DOF)	0.06
	3 DOF	12653		
30°	PRODAS	13801	-5 (DOF)	0.04
	3 DOF	13806		
45°	PRODAS	15396	-26 (DOF)	0.17
	3 DOF	15370		

Tabla N° 2: Comparación de alcances máximos.

Fuente: Elaboración propia.

Q°	Programa	Altura máxima (m)	Error (metros)	Error Relativo (%)
15°	PRODAS	841	+2 (DOF)	0.24
	3 DOF	843		
25°	PRODAS	1954	+5 (DOF)	0.26
	3 DOF	1959		
30°	PRODAS	2613	+5 (DOF)	0.19
	3 DOF	2618		
45°	PRODAS	4862	-8 (DOF)	0.16
	3 DOF	4854		

Tabla N° 4: Comparación de Alturas máximas.

Fuente: Elaboración propia.

Q°	Programa	Error por deflexión (m)	Error (metros)	Error Relativo (%)
15°	PRODAS	-90.16	+0.44 (DOF)	0.49
	3 DOF	-90.60		
25°	PRODAS	-206	-1 (DOF)	0.49
	3 DOF	-205		
30°	PRODAS	-277	-1 (DOF)	0.36
	3 DOF	-276		
45°	PRODAS	-548	+3 (DOF)	0.54
	3 DOF	-551		

Tabla N° 5: Comparación de Deflexiones máximas".
Fuente: Elaboración propia.

Q°	Programa	Tiempo de vuelo (seg)	Error (seg)	Error Relativo (%)
15°	PRODAS	25.64	-0.05 (DOF)	0.20
	3 DOF	25.59		
25°	PRODAS	38.77	-0.02 (DOF)	0.05
	3 DOF	38.75		
30°	PRODAS	44.89	+0.03 (DOF)	0.07
	3 DOF	44.92		
45°	PRODAS	61.85	-0.15 (DOF)	0.24
	3 DOF	61.70		

Tabla N° 6: Comparación de Máximos tiempos de vuelo.

Fuente: Elaboración propia.

Q°	Programa	Spin (Rad/seg.)	Error (Rad/seg.)	Error Relativo(%)
15°	PRODAS	969.80	+0.9 (DOF)	0.09
	3 DOF	970.70		
25°	PRODAS	903.09	+0.55 (DOF)	0.06
	3 DOF	903.64		
30°	PRODAS	881.01	+1.19 (DOF)	0.13
	3 DOF	882.20		
45°	PRODAS	850.56	-1.56 (DOF)	0.18
	3 DOF	849.00		

Tabla N° 7: Comparación de Spin final.

Fuente: Elaboración propia.

CONCLUSIONES

El desarrollo del modelo representativo de una trayectoria, contempla el manejo de una serie de factores, variables y constantes, los que en gran parte son referenciados en la bibliografía de manera conceptual, obviando el valor numérico que este representa para la formulación matemática. Lo anterior constituye un desafío importante para toda investigación relacionada al tema, debiendo apuntar los esfuerzos y estudios al análisis de trayectorias, además de la preparación y empleo de softwares de los cuales se requirió obtener información técnica de alta precisión y validez.

La validación de la formulación del modelo, adaptado del STANAG 4355, establece la base para la definición de un modelo de 3 DOF, de gran exactitud y precisión para estos calibres que cubren distancias inferiores a los 30 km.

Un modelo de trayectoria de 3 DOF es fácil de implementar y sus cálculos son menos intensivos que en un modelo superior de 6 DOF. La simplicidad del modelo 3 DOF implementado, permite una mayor comprensión de la mecánica en su trayectoria, produciendo a la vez resultados precisos.

El modelo obtuvo resultados generales muy próximos, a los datos previstos por las tablas de tiro entregadas por el Software PRODAS. Para trayectorias más tensas, con pequeños ángulos de elevación, el modelo de masa puntual modificado dio mejores resultados y menores tiempos de respuesta en su cálculo.

Un antecedente de ajuste, tiene que ver con el método numérico a emplear. En este caso se empleó un Runge Kutta de cuarto orden, método propuesto en gran parte de la bibliografía consultada, por ayudar a minimizar el almacenamiento en el computador y su gran efectividad en el cálculo de errores circulares. En este método se aplican también, ajustes para cada intervalo de cuadrante de elevación.

A partir de los datos del proyectil M 107 seleccionado, la información atmosférica y condiciones iniciales, el programa modularmente codificado resuelve las ecuaciones de forma iterativa, determinando las coordenadas de posición del proyectil para cada momento en el tiempo. Se llevó las simulaciones con diferentes etapas fijas de tiempo, para verificar la sensibilidad de la solución a los pasos mencionados. Las pruebas revelaron independencia (menos necesidad de ajustes) hacia el paso del tiempo de Dt = 0.01s.

LISTADO DE ABREVIATURAS Y ACRÓNIMOS

CD_{α^2}	Coeficiente de arrastre cuadrático (STANAG)
CD_o	Coeficiente de arrastre (STANAG)
CL_α	Coeficiente de elevación (STANAG)
CL_{α^3}	Coeficiente de elevación cúbico (STANAG)
CM_α	Coeficiente de momento de vuelco (STANAG)
CM_{α^3}	Coeficiente de momento de vuelco cúbico (STANAG)
CN_a	Coeficiente de elevación (PRODAS)
CN_{a^3}	Coeficiente de elevación cúbico (PRODAS)
C_{Spin}	Coeficiente de spin (STANAG)
CX_2	Coeficiente de arrastre cuadrático (PRODAS)

CX_o	Coeficiente de arrastre (PRODAS)
Cl_p	Coeficiente de spin (PRODAS)
Cm_q	Coeficiente de momento de vuelco (PRODAS)
Cm_{α^3}	Coeficiente de momento de vuelco cúbico (PRODAS)
C_{mag-f}	Coeficiente de Magnus (STANAG)
Cnp_α	Coeficiente de Magnus (PRODAS)
I_x	Momento axial de inercia
Q_M	Factor de ajuste Magnus
f_l	Factor del lift
g_o	Gravedad
α_e	Aproximación de "yaw" en reposo
c	Velocidad del sonido
DOF	Degree of freedom
DSA	Departamento de Sistemas de Armas
FAMAE	Fábrica y Maestranzas del Ejército de Chile
HE	High Explosive
IDIC	Instituto de Investigaciones y Control
M	Coeficiente de Mach
MPMTM	Modificated Point Mass Trajectory Model
NATO	North Atlantic Treaty Organization

ICAO	International Civil Aviation organization
O.E.	Objetivo Específico
PRODAS	Projectile Design and Analysis System
Q°	Cuadrante de elevación
R	Radio de la tierra
SAM	Sección Armamento y Municiones del Departamento Sistemas de Armas del IDIC
STANAG	Standardization Agreement
Λ	Vector de fuerza Coriolis
Ω	Velocidad angular de la tierra
QD	Factor de ajuste
d	Calibre del proyectil en milímetros
i	Factor de forma
p	Rotación axial del proyectil
v	Vector de la velocidad relativa del proyectil en el aire
w	Velocidad del aire respecto del suelo
π	Pi (3,1416)
ρ	Densidad del aire
v	Velocidad del proyectil
ω	Vector de rotación de la tierra

BIBLIOGRAFÍA

ARROW, Tech (1999). Manual del Usuario: versión 3.3.2. PC-PRODAS.

CARLUCCI, Jacobson (2008). Ballistics. EE.UU.: CRC Press.

CHAPRA (2012). *Applied Numerical Methods with MATLAB.* McGraw-hill.

CHEE, Meng (2006). Development of an Artillery Accuracy Model. EE.UU.: Naval Postgraduate School.

CUCHARERO (1992). Balística Exterior. España: Ministerio de Defensa.

DIVEDUC (2011). Guía para la redacción de citas bibliográficas. Santiago: División Educación.

FAB, Defense (2015). Catálogo 2015. Fab Defense.

GILLES, Brassard (1997). *Fundamentos de Algoritmia.* Prentice Hall.

GÓNZALEZ (2000). Funsamentos de Balística. Madrid: Ministerio de Defensa.

HERNÁNDEZ, R. (2008). Mecánica Técnica. Santiago: USACH.

HERNÁNDEZ, R.; FERNÁNDEZ, C. & BAPTISTA, P. (2006). *Metodología de la Investigación.* México D.F.: Infagon.

ISO 2533 (1975). The ISO Standard Atmosphere.

McCOY (1999). *Modern Exterior Ballistics.* Atglen: Schiffer Publishing.

OTAN (2009). The Modified Point Mass and Five Degrees of Freedom Trajectory Models. STANAG 4355 (Edition 3).

PETZOLD (1998). Computer Methods for Ordinary Differential Equations and Differential Algebraic Equations. SIAM: Society for Industrial and Applied Mathematics (July 31, 1998).

RAE (3 de septiembre de 2016). *Real Academia Española.* Obtenido de Real Academia Española: http://www.rae.es

REAL Regimiento de Artillería (2016). *Libro de Balística y Armamento Mayor.* Inglaterra.

RÍOS, Sixto (1999). *Modelización*. Madrid: Alianza.

Society for Industrial and Applied Mathematics. (1998). Effect of the mathematical model and integration step on the accuracy of the results of computation of artillery projectile flight parameters. Polonia: Faculty of Mechatronics and Aerospace, Military University of Technology.

HERRERA GARCÍA, Carlos. "Aplicación de un Modelo de Predicción para Trayectoria de Munición 155 mm estabilizada por Rotación". [Memoria para la obtención de Título]. Academia Politécnica Militar, Santiago de Chile, 2017.

LA AMENAZA DE LOS VEHÍCULOS AÉREOS NO TRIPULADOS Y ALTERNATIVAS DE MITIGACIÓN[1]

TENIENTE CORONEL PEDRO ZAMANILLO GÁLVEZ[2]

Resumen: *los drones o vehículos aéreos no tripulados (UAVs); en la actualidad abarcan tareas que van desde aspectos recreativos a un amplio espectro de usos en la defensa, industria, seguridad, agricultura, apoyo ante catástrofes, entre muchas otras aplicaciones; dentro de las cuales también está la de hacer un uso malicioso de esta tecnología. Este aspecto es analizado utilizando una metodología de categorización que segmenta la amenaza de acuerdo al nivel de peligro que representan; para luego proponer una metodología de mitigación por capas, que facilitan la neutralización de estas aeronaves, reduciendo al mismo tiempo el riesgo de generar daños colaterales.*

Palabras clave: *amenazas a la seguridad; drones, unmanned aerial vehicle o vehículo aéreo no tripulado (uav), medidas de mitigación, sensores y defensas.*

Abstract: *drones or unmanned aerial vehicles (UAVs); currently cover tasks that range from recreational aspects to a wide spectrum of uses in defense, industry, security, agriculture, disaster relief, among many other applications; within which is also the malicious use of this technology. This aspect is analyzed using a categorization methodology that segments the threat according to the level of danger they represent; then propose a mitigation methodology by layers, which facilitate the neutralization of these aircraft, while reducing the risk of generating collateral damage.*

Keywords: *threats to security, drones; UAVs, mitigation measures, sensors and defenses.*

INTRODUCCIÓN

El exponencial crecimiento que ha tenido el uso y desarrollo de aeronaves no tripuladas, está asociado al desarrollo creciente que tienen nuevas y numerosas aplicaciones que van encontrando en ellos otra dimensión para conseguir alcanzar objetivos que anteriormente era mucho más caro o excesivamente sofisticado lograr, generando nuevos estándares de eficiencia y oportunidad. Este

1 Artículo ganador del segundo puesto del concurso "Desarrollando Capacidades Militares", en el ámbito de Ciencia y Tecnología.

2 Ingeniero Politécnico Militar en Sistemas TICs. y Profesor de Academia en la asignatura de Mando y Control.

amplio abanico de ambientes en que participan de manera crítica, considera la vigilancia para la prevención de delitos, monitoreo en desastres y emergencias, combate contra la insurgencia, control de fronteras, cartografía, reconocimientos, inspección de infraestructuras remotas, servicios de entregas de servicios, extensión de arquitecturas de telecomunicaciones, operaciones de guerra electrónica, entre muchas otras.

Sin embargo, este crecimiento y el desarrollo de una tecnología que se ha vuelto alcanzable por casi cualquier persona que cuente con los recursos económicos y algunas habilidades motrices básicas, han generado también una dimensión negativa que acompaña a esta tecnología emergente; afectando la privacidad y seguridad tanto de particulares, como de organismos privados y estatales.

Los "Drones" o "Aeronaves no tripuladas" consisten esencialmente en un vehículo aéreo que no requiere de una tripulación debido a que es controlado remotamente, opera bajo parámetros de guiado preprogramado por software o realiza su vuelo bajo el control de robots.

Desde una perspectiva militar, el espíritu original que rodeaba al empleo de este tipo de aeronaves, era el de realizar tareas bajo situaciones de alto riesgo o en territorios hostiles sin exponer a las tripulaciones. Actualmente, su empleo también se ha diversificado, incluyendo vigilancia y reconocimiento, detección de campos minados y muchas otras tareas de combate o apoyo al combate; volviéndose especialmente necesario para conseguir una mayor eficiencia en el uso de los recursos de las diferentes Fuerzas Armadas para enfrentar exitosamente las tareas de sus diferentes áreas de misión. Para enfrentar estos requerimientos se ha generado una diversificación de formatos y capacidades que va desde grandes aeronaves, que requieren de una infraestructura y tripulaciones que les permiten ejecutar misiones a grandes alturas y con una extensa autonomía de vuelo (en que incluso se efectúan relevos de las "tripulaciones" durante el cumplimiento de la misión), hasta otros que por sus pequeñas dimensiones son denominados MICRO UAVs para el cumplimiento de tareas que requieren de sigilo dentro de un alcance y alturas acotados.

La reciente masificación de este tipo de aeronaves en formatos económicos y pequeños, pero con importantes prestaciones en sus capacidades de carga, de obtención de imágenes y de bajada de datos; los convierten también en nuevas amenazas que pueden ser aprovechadas por su facilidad para evadir medidas convencionales de seguridad y vigilancia, lo que facilita el incorporarles cargas explosivas convirtiéndolos en dispositivos explosivos improvisados (IEDs), como plataformas para acciones de obtención de imágenes e información confidencial o crítica (espionaje) desde recintos o propiedades con acceso restringido.

El propósito de este artículo es describir algunas medidas de mitigación que forman parte de las mejores prácticas y el estado del arte en cuanto a las contramedidas existentes.

TIPOS DE AERONAVES NO TRIPULADAS

Cuando hacemos referencia a las aeronaves no tripuladas, la primera particularidad con la que nos encontramos es con la existencia de varios acrónimos y abreviaturas tales como DRON, DRONE, UAV, UAS, RPA y RPAS.

Es por esta razón que comenzaremos describiendo las particularidades de cada uno de tal manera de identificar sus particularidades y diferencias.

- *Drone* o *dron* (en español): su traducción desde el inglés, literalmente significa zángano (abeja macho), en aeronáutica se usa para denominar los vehículos aéreos no tripulados. Este término aún no ha sido reconocido por la Real Academia de la Lengua Española, por lo que no existe oficialmente.
- UAV *(Unmanned Aerial Vehicle):* vehículo aéreo no tripulado.
- UAS *(Unmanned Aerial System):* sistema aéreo no tripulado, es decir la aeronave no tripulada junto a su sistema de control.
- UCAV *(Unmanned Combat Aerial Vehicle):* vehículo aéreo de combate no tripulado, es decir, un UAV con capacidades para atacar objetivos (usualmente terrestres).
- RPA *(Remotely Piloted Aircraft):* aeronave controlada de forma remota. Este concepto surgió como una especie de "eufemismo" en EE.UU., para diferenciarlos de aquellas aeronaves de aplicación militar y aclarar al mismo tiempo, la existencia de una persona a cargo de controlar el vehículo y evitar accidentes (daños a terceros) en caso de desperfectos durante el vuelo.
- RPAS *(Remotely Piloted Aircraft System):* sistema aéreo tripulado de forma remota, el que además del vehículo, considera sus dispositivos de control, tripulación y/o soporte en forma integral.

Usualmente los conceptos Drone, UAV, UAS y UCAV, son denominaciones para aparatos y/o sistemas asociados a aplicaciones militares, mientras que los conceptos RPA y RPAS son denominaciones utilizadas en el ámbito civil, tal como lo declara y norma en nuestro país la DGAC (Dirección General de Aeronáutica Civil), a través de la Norma Técnica DAN 91 "Reglas del Aire", y de la DAN 151 (2ª Edición), "Operaciones de Aeronaves Pilotadas a Distancia (RPAS) en Asuntos de Interés Público, que se efectúen sobre Áreas Pobladas".

En este sentido es importante resaltar que la totalidad de los RPAs son UAVs, es decir, vehículos aéreos no tripulados; pero por el contrario los UAVs no son necesariamente RPAs, ya que para entrar en esta designación deben ser controlados por una persona.

CLASIFICACIÓN MILITAR DE AERONAVES NO TRIPULADAS

Si bien no existe un consenso para generar un estándar universal en la categorización de estos ingenios; al efectuar una búsqueda acerca de la clasificación militar que se da a las

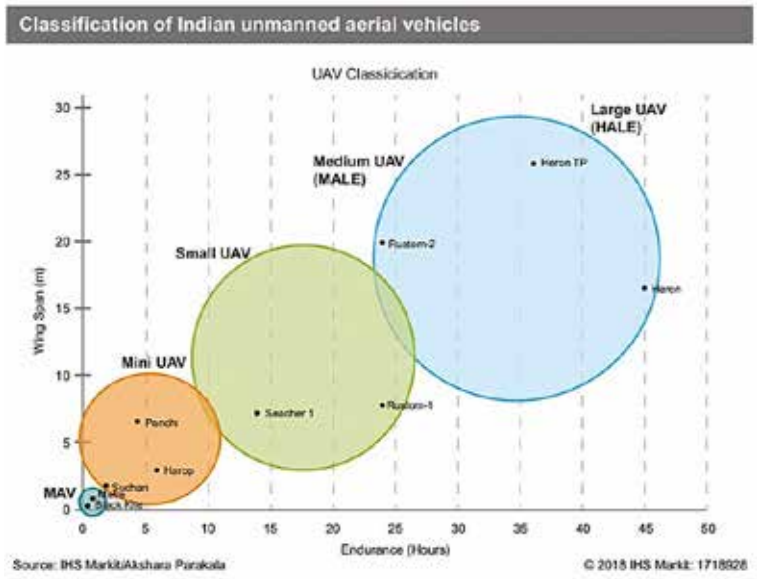
aeronaves no tripuladas, nos encontramos con que una de las más aceptadas, está asociada a la definida (por efectos prácticos) por las organizaciones militares integrantes de la OTAN, en conjunto con la industria militar de las naciones que participan en la misma, como a continuación se detalla:

- HALE UAV *(High Altitude Long Endurance):*[3] sistema aéreo no tripulado con capacidad de operar de manera óptima a una elevada altitud (a partir de los 30.000 pies) con una gran autonomía (se considera a partir de 32 h o más). Ejemplo: Northrop Grumman RQ-4 Global Hawk.[4]
- MALE UAV *(Medium Altitude Long Endurance):*[5] Sistema aéreo no tripulado con capacidad de operar de manera óptima a una altitud que oscila entre los 10.000 y los 30.000 pies con una autonomía que normalmente abarca entre 24 h y 48 h. Ejemplo: Elbit Systems Hermes 900 Kochav (Star).[6]
- SMALL UAV *(SUAV o UAV miniatura):* vehículo aéreo no tripulado lo suficientemente pequeño para ser lanzado y transportado por un solo operador (su peso máximo fluctúa entre los 20 y 25 kg aprox. según diferentes normas y desarrolladores).[7]
- MICRO UAV *(MUAV):* vehículo aéreo no tripulado lo suficientemente pequeño para ser llevado en una mano. Sus reducidas dimensiones presentan como contraparte una autonomía y alcances muy reducidos, además de una alta sensibilidad a factores meteorológicos.[8]
- NANO UAV *(NAV o UAV nanométrico):* vehículo aéreo no tripulado de características experimentales y dimensiones inferiores a los 7 cm.

Su diminuto tamaño lo circunscribe al cumplimiento de tareas de reconocimiento en interiores, bajo una silueta que le permita asemejarse a algún organismo vivo como aves pequeñas.

Sin embargo esta misma restricción en dimensiones implica la limitación de contar con una cantidad excesivamente pequeña de energía para volar, lo que mantiene actualmente a los prototipos en un rango de tiempos de operación que rodea los 15 minutos.[9]

3 En español, Alta Altitud Larga Duración.
4 http://www.northropgrumman.com/Capabilities/GlobalHawk/Pages/default.aspx
5 En español, Mediana Altitud Larga Duración.
6 https://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=1236
7 http://www.natick.army.mil/soldier/media/fact/techprog/SUAVs.htm
8 https://www.theengineer.co.uk/issues/aerospace-and-defence-2013/the-rise-of-the-micro-air-vehicle/
9 http://www.darpa.mil/dso/thrusts/materials/multfunmat/nav/index.htm



Clasificación de aeronaves no tripuladas de las fuerzas de defensa e industria militar de la India.
Fuente: PARAKALA, Akshara. Flying high: India's indigenous UAV programmes spread their wings. *Jane's International Defence Review,* march 2018, p. 55.

AMENAZAS A LA SEGURIDAD

El amplio y creciente mercado de los UAVs, con todo tipo de modelos, tamaños, prestaciones y capacidades a costos cada vez más asequibles por cualquiera ha llevado a que de forma involuntaria o intencionadamente, se generen incidentes que reflejan la problemática a la seguridad que estos aparatos representan, generando una especial preocupación por parte de gobiernos y organismos de seguridad como una materia que resulta compleja de regular y de fiscalizar; así es como en septiembre de 2013, un dron cayó a pocos metros de la canciller alemana, Angela Merkel, durante un mitin político en Dresden, Alemania,[10] en abril de 2015 un dron aterrizó con un contenedor con arena radioactiva en la residencia oficial del primer ministro de Japón, Shinzo Abe, donde además el responsable señaló que lo habría hecho *"para demostrar que se podía hacer"*,[11] en febrero de 2018 en EE.UU. se produjo el que sería el primer accidente aéreo causado por un dron que no habría respetado la norma de altura para su uso por particulares[12] y en julio de 2018 un dron con granadas de fragmentación realizó un ataque contra la casa del secretario de Seguridad Pública de Baja California en México, Gerardo Sosa Olachea. Estos eventos demuestran y respaldan su potencial

10 https://www.24horas.cl/internacional/un-drone-asusta-a-merkel-durante-acto-de-campana-844109
11 http://www.emol.com/noticias/internacional/2015/04/25/714192/japon-cae-sujeto-que-poso-dron-con-trazas-de-radioactividad-en-oficina-del-primer-ministro.html
12 https://www.latercera.com/tendencias/noticia/investigan-posible-accidente-aereo-causado - dron-ee-uu/72349/

para vulnerar sistemas de seguridad convencionales e incluso otros no tan convencionales como ocurrió en el 2015, cuando los avanzados sistemas de detección de aeronaves y misiles de la Casa Blanca fueron evadidos por un dron que no tuvo mayores problemas para ingresar y estrellarse en uno de sus jardines.[13]

Todos estos hechos, si bien no dejaron víctimas que lamentar, son una advertencia de la amenaza que pueden representar los UAVs, al ser utilizado por organizaciones subversivas, grupos de insurgentes o incluso fuerzas irregulares beligerantes en el contexto de una crisis y/o conflictos de baja intensidad, como ha sido el caso de la guerra civil en Ucrania, donde desde el inicio de las hostilidades en 2014, se han registrado casos de participación de drones de características civiles y militares en diferentes tipos de tareas de apoyo a las diferentes facciones en conflicto.[14]

Por otra parte, como se puede apreciar de sus potencialidades, podemos concluir que algunos de sus principales atributos son:

- Gran versatilidad que otorgan al poder preparar sitios de lanzamiento o despegue de manera encubierta sin una gran preparación previa y con una alta disponibilidad de lugares alternativos para efectuar aterrizajes.
- Una elevada capacidad para observar y/o atacar objetivos difíciles o peligrosos de alcanzar por vía terrestre.
- Capacidad para evadir defensas aéreas y la observación desde tierra.
- Dificultad para determinar el propósito con el que están siendo utilizadas las aeronaves (si es para uso recreacional, activismo, obtención de noticias, entregas de encomiendas, narcotráfico, actividades subversivas, etc.).
- Elevada capacidad para transportar cargas que puedan lanzarse contra instalaciones y/o personas (tales como propaganda, agentes químicos, explosivos, etc.).
- Posibilidad de alcanzar objetivos a diversas distancias con una precisión más que aceptable para la mayoría de las tareas existentes en el ámbito militar.
- Elevada eficiencia de costos en contraste con otros sistemas tripulados por humanos e incluso con algunos sistemas de misiles.
- Y un elevado impacto psicológico sobre las potenciales víctimas y medios de comunicación, que puede llevar al desencadenamiento de diferentes efectos según sea el interés y propósito de quien los utilice.

Adicionalmente, a todas las capacidades señaladas en el ámbito de la subversión e insurgencia, se suman las capacidades que existen y se están desarrollando en el ámbito militar, los

13 https://clipset.20minutos.es/un-drone-se-estrella-en-la-casa-blanca-y-activa-la-alerta-de-seguridad/

14 http://www.seguridadinternacional.es/revista/?q=content/el-papel-de-rusia-en-el-conflicto-de-ucrania-%C2%BFla-guerra-h%C3%ADbrida-de-las-grandes-potencias

que van desde el más conocido reconocimiento con aeronaves de gran autonomía y capacidades electroópticas por medio de sistemas FLIR[15] (infrarrojo de barrido frontal) o de grabación de imágenes, pasando por aeronaves con revestimientos o pinturas que les permitan disminuir aún más su "firma electrónica" ante sensores (radares) enemigos para el cumplimiento de tareas de apoyo de combate.

Otros cuentan con "targeting pods" que consisten en sensores para la detección y selección de blancos, donde adicionalmente pueden participar en el guiado de municiones guiadas de precisión (PGM),[16] otros ya están incorporando módulos de localización desde una estación (SSL)[17] para el apoyo a las operaciones de guerra electrónica por medio de sistemas de radiolocalización de emisores tanto de comunicaciones como radáricos y/o efectuar levantamientos radioeléctricos de emisores en zonas de interés, para la entrega de elementos de vida y combate a unidades geográficamente aisladas o difíciles de abastecer por otros medios.

Finalmente al desarrollo de UAVs con cargas explosivas de diferentes magnitudes que cuentan con la capacidad para determinar su blanco a base de algoritmos de identificación y selección (que pueden variar desde firmas electrónicas, registros de calor a señales de telefonía celular para equipos específicos entre otros criterios), lo que les permite encontrarlos y detonarse contra ellos independientemente de si se encuentran estáticos o en movimiento, así como si corresponden a individuos, vehículos o infraestructuras.

Un estudio realizado para el Departamento de Seguridad Nacional de Estados Unidos (DHS)[18] para enfrentar las amenazas por UAVs, denominado *"Statement on the security threat posed by unmanned aerial systems and possible countermeasures"*,[19] plantea una categorización de acuerdo a su nivel de sofisticación y la intención de sus operadores, que utilizaremos para describir en adelante los niveles de amenaza que representa cada uno de ellos:

- 1ª Categoría: intrusiones accidentales, sin importar el grado de sofisticación del operador.
- 2ª Categoría: intrusiones intencionales por operadores no sofisticados.
- 3ª Categoría: intrusiones intencionales por operadores sofisticados que son capaces de ensamblar sus propios UAVs a partir de sus componentes, además de modificar su software y/o hardware a voluntad.

15 Del ingles, *Forward Looking InfraRed*.
16 Del ingles, *Precision Guided Munitions*.
17 Del ingles, *Single Station Location*.
18 Del ingles, *United States Department of Homeland Security*.
19 HUMPHREYS T., *Statement on the security threat posed by unmanned aerial systems and possible countermeasures*. Statement to the Subcommittee on Oversight and Management Efficiency of the House Committee on Homeland Security, 18 Marzo 2015, Washington DC, EE.UU., 2015.

Para enfrentar a las amenazas UAV presentes en las primeras dos categorías de esta clasificación, existen contramedidas tecnológicas que pueden mitigar sus efectos, permitiendo en algunos casos su captura o neutralización.

Sin embargo esta situación cambia en la última en virtud de las contramedidas que pueden ser implementadas por los potenciales atacantes que cuenten con una preparación técnica que les permita generar sus propias aeronaves o efectuar modificaciones relevantes a UAVs convencionales, como por ejemplo un atacante que desee realizar un atentado del tipo kamikaze contra un objetivo de interés, podría simplemente agregar una carga explosiva ligera a un UAV de ala fija y generar el despegue desde una distancia significativa que le permita mantener el control sin comprometerlo.

Podría evadir los sensores acústicos simplemente apagando el motor en la trayectoria final al objetivo; los radares de detección podrían evadirse empleando en la construcción de la aeronave "materiales absorbentes" con una baja reflexión de las emisiones de radar (Ej. Gomaespuma),[20] que permitan reducir la Sección Recta Radar.[21] Adicionalmente, el UAV se podría configurar para ignorar y dejar de emitir señales de radiofrecuencia durante la trayectoria final de vuelo (silencio radial), así como configurar su piloto automático para "desactivar" o ignorar las señales del Global Navegation Satellite System (GNSS) en su aproximación final al objetivo, convirtiendo a esta aeronave en una amenaza muy difícil de detectar y neutralizar.

En virtud de lo anterior, se propone una respuesta por capas, que se encuentra basada en las soluciones y desarrollos que han demostrado ser los más eficientes con los que cuenta la industria actualmente.

CAPAS DE MITIGACIÓN

A continuación, realizaremos una rápida descripción de diferentes tecnologías que permiten mitigar o neutralizar la acción de algunas amenazas UAV considerando una metodología a base de capas que consisten en:

- Zonas Restringidas Georreferenciadas (Geofencing).[22]
- Detección.
  - Sensores de emisiones de radiofrecuencias.
  - Sensores Electroópticos.
  - Sensores Acústicos.
  - Radares.

20 http://academica-e.unavarra.es/bitstream/handle/2454/7548/578085.pdf?sequence=1
21 Se refiere a la "firma" o "superficie" que es detectada por el radar, a base de la cantidad de energía reflejada por el objeto o blanco.
22 En español es traducido como "Geovallado o Geocerco".

- Defensa Electrónica.
  Perturbación al enlace de control (Jamming)[23] y Apropiación de la aeronave (Hijacking).[24]
  Perturbación al Sistema Global de Navegación por Satélite (GNSS) y Suplantación de GNSS (Spoofing).
- Defensa Cinética.

Es importante considerar que, para incrementar la efectividad en la mitigación de amenazas a niveles aceptables, deben combinarse las capacidades de diferentes capas, considerándose imprescindible, el contar con algún sistema de detección (capa 2) que sea idealmente autónomo con el fin de eliminar el fallo humano y mejorar la cobertura.

Zonas restringidas georreferenciadas (geofencing)

Corresponde a zonas que se encuentran restringidas para el tránsito (vuelo) de Aeronaves No Tripuladas que no se encuentren autorizadas, estas zonas son señaladas (marcadas) por medio de técnicas de posicionamiento espacial que dan a la zona que se encuentra restringida, una localización geográfica única y claramente definida en un sistema de coordenadas y datum específicos; estos sectores son establecidos por entidades gubernamentales (como autoridades reguladoras del tránsito aéreo) y transmitidas a los desarrolladores o proveedores de drones que son comercializados dentro de los respectivos países donde son comercializados, con el propósito de que estos ingresen las restricciones dentro del conjunto de parámetros de vuelo (estableciéndolas como una restricción predefinida por defecto), impidiendo así que sus aparatos ingresen de manera voluntaria o accidental en áreas en que pudiesen causar conflictos con la seguridad (Ejemplo: aeropuertos, instalaciones gubernamentales, zonas de entrenamiento militar, etc.).

Este tipo de medidas son aplicables a aeronaves que incorporan dentro de su sistema de navegación algún Servicios Basados en Localización (LBS)[25] o Servicios Basados en Servicios de Información Dependientes de la Localización (LDIS).[26]

Detección

Sensores de emisiones de radiofrecuencias, consisten en equipos que cuentan con la capacidad para detectar las emisiones de paquetes de datos que habitualmente son enviados por los drones a sus estaciones de control en tierra, permitiendo efectuar una estimación de la posición de la aeronave y en algunos casos, de su controlador. Dependiendo su nivel de desarrollo, puede asociar

23 En español se traduce como “interferencia”.
24 En español se traduce como “secuestro”.
25 Del inglés, *Location Based Services*.
26 Del inglés, *Location Dependent Information Services*.

los identificadores en las señales transmitidas entre el UAV y su estación de control, logrando constituir un medio de segregación entre la aeronave y el control en tierra de la amenaza de otros UAVs y sus controladores en una misma área de empleo (puede además constituir un medio de prueba en caso de que se produzca una transgresión a la legalidad por parte de alguna aeronave). Pueden ser evadidos por medio de "silencio radial" entre la estación control y la aeronave.

Sensores electroópticos, consisten en equipos que pueden detectar Vehículos Aéreos No Tripulados, por medio de la combinación de cámaras ópticas con cámaras térmicas; esto se logra técnicamente por intermedio de instrumentos pasivos de captación de imágenes que miden la radiación óptica (energía lumínica) o registros de calor, transformando los cambios percibidos por el receptor, en un registro de señales eléctricas medibles que son interpretadas en monitores como objetos,[27] permitiendo la detección diurna. En el caso de detecciones nocturnas, esta se logra por medio de la asociación de cámaras ópticas con sensores infrarrojos (IR)[28] y/o con cámaras térmicas. Presentan la limitación de que las cámaras ópticas, en ocasiones, tienen problemas para distinguir entre drones y animales voladores; razón por la cual se les debe asociar a computadores con software de identificación el cual consiste en algoritmos que analizan las trayectorias para determinar la naturaleza del objetivo detectado (normalmente los seres vivos presentan trayectorias mucho más irregulares que las de los UAVs).

Sensores acústicos, consiste en sistemas que por medio de la asociación del sonido de los sistemas de vuelo de los drones, que se encuentran almacenados en bibliotecas de sonidos, permiten la identificación del modelo y características de las aeronaves que se encuentren consideradas en ellas.[29] Esta tecnología depende de formar una red de sensores acústicos que generen una capacidad para detectar los sonidos producidos por un dron a distancias que podrían llegar hasta 500 metros de distancia. Sin embargo, cabe señalar que es inefectivo en áreas urbanas con una alta saturación acústica (ruido ambiente) y puede ser engañado por medio de la reproducción de grabaciones de audio con el sonido de rotores de UAVs.

Radares, consiste en una generación de sensores que surgen como alternativa de solución ante la alta tasa de falsos positivos que se observaban con el empleo de radares convencionales y que eran concebidos como consecuencia de la detección de aves y otros vectores que forman parte de la fauna propia de las regiones donde eran utilizados. Esta situación generó la necesidad de desarrollar radares de alta fidelidad que permiten la detección de aeronaves no tripuladas, por medio de la utilización de los denominados Microrradares de ondas milimétricas,[30] los que consisten en sistemas de radares activos de alta resolución y que pese a tener un radio de acción reducido a

27 BOREMAN, Glenn D. (1999). *Fundamentos de electro óptica para ingenieros,* Washington DC, EEUU., SPIE Press, p. 55.
28 Del inglés, *Infrared Radiation*.
29 https://www.droneshield.com/how-droneshield-works/
30 https://www.fhr.fraunhofer.de/en/businessunits/security/Detection-of-small-drones-with-millimeter-wave-radar.html

algunos cientos de metros, permiten mantener una conciencia situacional persistente ante este tipo de amenazas, aunque requieren de personal entrenado que sea capaz de distinguir entre UAVs y otros elementos que pudiesen encontrarse en el aire.

Defensa electrónica

Perturbación del Enlace de Control (Command Link Jamming)[31] y Apropiación de la aeronave (Hijacking),[32] consiste en aprovechar el fenómeno de debilitamiento de la señal que recibe el UAV en la medida en que este se aleja de su estación de control en tierra y al mismo tiempo aprovecha el efecto inverso en que a medida que la aeronave se aproxima a un emisor que "emula" los parámetros de comunicaciones de su estación de control, los que dependiendo de su sofisticación tecnológica permiten:

- Emitir instrucciones bajo los mismos parámetros y frecuencia que utiliza su control en tierra para capturar el control de la aeronave.
- Perturbar la señal enviada por el control en tierra, neutralizando sus comunicaciones y anulando la posibilidad de que la aeronave pueda recibir nuevas instrucciones.
- Es relevante mencionar que el desarrollo de capacidades para apoderarse del control de UAVs, por medio de señales que imiten las de su legítimo control terrestre por parte de potenciales atacantes; permitiría a estos últimos, contar con la capacidad para interferir y utilizar aeronaves en vuelo que no les pertenecen, lo que podría ser aprovechado para cumplir sus propios objetivos. Es por este mismo aspecto que se vuelve relevante el que los UAVs que entren en servicio, ya sea como sistema autónomo o complemento de sistemas de armas de las Fuerzas Armadas, cuenten con sistemas de encriptación para resguardar sus comunicaciones.

Perturbación al GNSS[33] y Suplantación de GNSS (Spoofing), consiste en generar emisiones compatibles con las señales recibidas por los UAVs desde el Sistema Global de Navegación por Satélite que utilicen para identificar su ubicación dentro de la zona geográfica en la que se están empleando, lo que crea un conjunto de parámetros equivocados que generan un error en su Sistema Global de Navegación por Satélite (GNSS) desviándolos de la trayectoria programada.

Es relevante señalar que este tipo de medidas podría generar daños colaterales como: impedir a otras aeronaves sobrevolar el área donde se está generando la perturbación o suplantación, además de afectar a los sistemas de navegación de vehículos terrestres, torres y equipos de telefonía celular e incluso algunos soportes a la aeronavegación en naves tripuladas, entre otros.

31 En español se traduce como "Interferencia al enlace de comando".
32 En español se traduce como "secuestro".
33 GNSS, es un término genérico que engloba a todos los sistemas de posicionamiento tales como GLONASS, GPS, Galileo, Beidou, etc.

Defensa cinética

Consiste en la aplicación de una medida que tiene un efecto físico sobre la aeronave que se desea neutralizar.

La experiencia ha demostrado que muchos de los sistemas en uso dentro de las diferentes Fuerzas Armadas y de Orden Público de diferentes naciones, tales como armas de fuego, municiones inteligentes, pequeños misiles guiados y sistemas de armas láser, logran el efecto neutralizador sobre las frágiles estructuras de los drones, sin embargo su elevada tasa de fallas y la siempre presente posibilidad de generar daños colaterales graves sobre la población (especialmente en ambientes urbanos que es donde se evidencian con mayor frecuencia estas amenazas), hacen la mayoría de las veces inviable el empleo de estas medidas.

Lo anterior ha llevado al desarrollo de otras soluciones como el empleo de "Interceptores de UAVs", los que consisten básicamente en un dron de una envergadura y potencia tales, que les permita desplazarse rápidamente hacia la trayectoria de la amenaza, para atraparla con una red especialmente diseñada con ese propósito. Y aunque se puede afirmar que esta es una tecnología que aún no alcanza un apropiado nivel de madurez, hasta el momento se ha mostrado muy efectiva y con la ventaja adicional de que permite retener a la aeronave como prueba física de la violación del espacio aéreo restringido.

Por otra parte, también esta tecnología se ha adaptado a sistemas de lanzamiento de redes portátiles por medio de plataformas similares a las de los lanzacohetes, que por medio de un lanzador que no supera los 10 kg, permiten abatir drones a distancias de hasta 100 metros.[34]

Finalmente, es importante señalar que, el empleo de las medidas de mitigación descritas requieren de una cuidadosa planificación donde se identifique claramente a los activos que se desea resguardar, así como la mejor manera de explotar al máximo las capacidades presentes en las diferentes capas, por medio de la determinación de posibles trayectorias de aproximación, los escenarios y amenazas más peligrosas y la mejor manera de explotar las propias capacidades integrándolas de manera sinérgica.

CONCLUSIÓN

El presente artículo busca entregar una evaluación acerca de las diferentes características que enmarcan a los UAVs o drones como una amenaza emergente, y que pese a no ser una tecnología completamente madura, ya se encuentra presente en diversos entornos donde se le da desde un

34 https://openworksengineering.com/skywall

uso puramente recreacional, pasando por entregas de encomiendas, obtención de noticias, control de uso de vías urbanas y lucha contra la delincuencia hasta su contraparte en la participación en activismo por diferentes causas, narcotráfico, actividades subversivas, etc.

Esta situación no es ajena a las Fuerzas Armadas y en particular al Ejército, el que representa un codiciado objetivo no solo por la información que pueda ser capturada por naciones con un interés por conocer sus medios, capacidades o empleo de sus fuerzas, sino también por activistas que busquen causar algún tipo de incidente que puedan utilizar para sus propósitos e intereses, así como por particulares a quienes les pudiese resultar interesante vulnerar la seguridad militar por el solo hecho de enfrentarlo como un reto o desafío personal.

Es por lo anterior que adicionalmente se presenta una categorización de diferentes niveles de amenaza, basada en las intenciones y el nivel de capacitación de sus operadores; para, finalmente, entregar una proposición de metodología por capas de protección, donde se señalan las características y algunas de las vulnerabilidades presentes en las diferentes medidas de mitigación expuestas.

BIBLIOGRAFÍA

BOREMAN, Glenn D. (1999). *Fundamentos de electro óptica para ingenieros*, Washington DC, EE.UU., SPIE Press, p. 55.

HUMPHREYS, T., Statement on the security threat posed by unmanned aerial systems and possible countermeasures. Statement to the Subcommittee on Oversight and Management Efficiency of the House Committee on Homeland Security, Washington DC., EE.UU., 18 marzo 2015.

http://academica-e.unavarra.es/bitstream/handle/2454/7548/578085.pdf?sequence =1

http://www.darpa.mil/dso/thrusts/materials/multfunmat/nav/index.htm

http://www.emol.com/noticias/internacional/2015/04/25/714192/japon-cae-sujeto-que-poso-dron-con-trazas-de-radioactividad-en-oficina-del-primer-ministro.html

http://www.natick.army.mil/soldier/media/fact/techprog/SUAVs.htm

http://www.northropgrumman.com/Capabilities/GlobalHawk/Pages/default.aspx

http://www.seguridadinternacional.es/revista/?q=content/el-papel-de-rusia-en-el-conflicto-de-ucrania-%C2%BFla-guerra-h%C3%ADbrida-de-las-grandes-potencias

https://clipset.20minutos.es/un-drone-se-estrella-en-la-casa-blanca-y-activa-la-alerta-de-seguridad/

https://openworksengineering.com/skywall

https://www.24horas.cl/internacional/un-drone-asusta-a-merkel-durante-acto-de-campana-844109

https://www.droneshield.com/how-droneshield-works/

https://www.fhr.fraunhofer.de/en/businessunits/security/Detection-of-small-drones-with-millimeter-wave-radar.html

https://www.latercera.com/tendencias/noticia/investigan-posible-accidente-aereo-causado-dron-ee-uu/72349/

https://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=1236

https://www.theengineer.co.uk/issues/aerospace-and-defence-2013/the-rise-of-the-micro-air-vehicle/

DISEÑO DE UN SISTEMA DE APOYO AL CONDUCTOR ANTE MANIOBRAS EN REVERSA DEL TANQUE LEOPARD 2A4[1]

MAYOR ERNESTO NEBREDA LE ROY[2]

RESUMEN: *en este artículo se realizará un análisis de las experiencias aplicadas por otros ejércitos en sus tanques principales de batalla, para realizar la proposición de integración de un sistema de apoyo al conductor ante maniobras en reversa del tanque Leopard 2A4, de producción nacional, que permita entregar un ángulo de visión de la parte trasera del tanque, logrando así aumentar la seguridad en las maniobras en reversa de este tanque de combate y, a su vez, permitir explorar la sensorización de este vehículo.*
Palabras clave: *tanque, sensor, cámara, conductor, demostrador tecnológico.*

ABSTRACT: *in this article will described an analysis of the experiences applied by other armies in their main battle tanks, to make the proposition of integration of a support system for the driver before he maneuvers in reverse of the Leopard 2A4 tank national production which will provide an angle of view to the driver of the tank rear tank, it will increas the safety in the reverse maneuvers of this tank and in it will be able to explore the sensorization of this vehicle.*
Keywords: *tank, sensor, camera, driver, technological demonstrator.*

INTRODUCCIÓN

En el campo de batalla moderno existe una tendencia a nivel mundial de buscar la mejora del rendimiento de las capacidades técnicas de los tanques principales de batalla en cuanto a movilidad, letalidad y protección, la que se busca obtener a través de la integración de sistemas conformados por sensores. Esto es logrado con la implementación de sistemas como el de defensa activa o los sistemas de conciencia situacional tanto para permitir mejorar las capacidades de la tripulación, como del escalón superior.[3]

---

1 Artículo ganador del tercer puesto del concurso "Desarrollando Capacidades Militares", en el ámbito de Ciencia y Tecnología.
2 Ingeniero Politécnico Militar en Sistemas Logísticos, mención Mantenimiento.
3 PHILIPS, Malcom. "Main Battle Tank Update", *Military Technology*, p. 106, junio 2012.

Dentro de los sistemas que emplean sensores podemos ver los de blindaje activo implementados como sistema de protección activo SPA 360° de Rheinmetall, el IronFisty y Thropy.[4]

Se destacan también sensores como radares de campo de batalla, sistemas de identificación amigo enemigo, sistemas de detección lasérico, sistemas de detección de radar y sistemas remotos de control de armamento secundario.

Cabe destacar que existen en la industria internacional sistemas realizados en el tanque Leopard 2A4 como el sistema de protección activa SPA 270° y SPA 360° realizado por la Rheinmetall y los sistemas de detección de emisiones láser desarrollado por la KMW. El sistema de detección láser capta las emisiones láser, las clasifica e identifica con información sobre el azimut y elevación del punto de disparo y se encuentra incorporado al software de mando y control del tanque.

Lo anterior lleva a plantear la necesidad de realizar integración de sistemas basados en sensores a nuestro principal tanque de combate (tanque Leopard 2A4) a un bajo costo y desarrollados en Chile.

Este se propone como un sistema denominado, sistema de apoyo al conductor ante maniobras en reversa, el que busca entregar al conductor un ángulo de visión de la parte posterior del tanque, proveyendo la capacidad de poder discernir sobre los obstáculos existentes en la parte posterior del tanque Leopard 2A4, a fin de evitar la ocurrencia de accidentes.

METODOLOGÍA

En esta investigación se aplicó la metodología de ingeniería de sistemas y, en su primera etapa, se determinó el problema a solucionar, el que se estableció como deficiente campo de vista del conductor de la parte posterior del tanque Leopard 2A4.

Luego se inició un análisis de los sistemas civiles existentes, la experiencia que han tenido otros ejércitos en cuanto a la integración de sistemas de apoyo a la conducción ante maniobras en reversa, el análisis de los sistemas a nivel mundial y la solicitud de antecedentes a los *stakeholders* de tanque Leopard 2A4, para así levantar los requerimientos de este sistema, generar un modelo físico y, finalmente, un demostrador tecnológico que busque solucionar el problema planteado en forma parcial, adaptando los sistemas estudiados a nuestra realidad nacional, ya que será realizado con componentes de fácil adquisición y reposición.

4 Israel defense (en línea), ROJKES, Ami (2016). El Trophy Rafael y el IronFist de IMI están en el blanco, disponible en www.israeldefense.com, Israel.

DESARROLLO

Sistemas de uso civil

Para enfocarnos a buscar soluciones aplicables, se realizará un análisis del área de vehículos civiles donde se puede encontrar una variedad de sistemas de sensores que son empleados en el apoyo de la conducción en maniobras en reversa de los conductores de vehículos livianos y de alto tonelaje como camiones mineros. Se iniciará este análisis por los sistemas de cintas magnéticas que emplean cintas con magnetismo, como su nombre lo dice, a través de inducción, usadas, generalmente, en sistema de vehículos que cuentan con parachoques plásticos, ya que actúan en forma direccional por inducción, lo que no las hace muy aptas para ser empleadas en tanques o vehículos blindados.

Luego tenemos los sensores de proximidad muy conocidos por su empleo en los autos. Este emplea sensores de ultrasonido para poder detectar algún tipo de obstáculo en la parte trasera del vehículo. En algunos autos se emplea incluso en los puntos muertos para así alertar al conductor de la existencia de un vehículo u objeto ocupando los ángulos muertos de visión. Son de fácil instalación y existe una gran gama de ellos. La desventaja es que no se puede discernir si el objeto producirá daño al vehículo, pudiendo ser tan solo, por ejemplo, una hoja lo que alertaría de la existencia de un objeto en la parte posterior del vehículo, pero no representa un real obstáculo para este.

A su vez, también se encuentran disponibles una gran gama de sensores de ultrasonido para los diferentes tipos de procesadores, como el Arduino, el Raspberry, y otros que se encuentran disponibles en el mercado y son utilizados, ya sea en sistemas de avance o retroceso de sistemas autónomos.

Luego encontramos la gran variedad de cámaras existentes lo que se hace bastante interesante, debido a que gran parte de los vehículos emplea cámaras de retroceso y no sensores, ya que estas entregan la capacidad al conductor de discernir qué es lo que hay en la parte trasera del vehículo, determinar si ese objeto presenta un verdadero obstáculo para el vehículo, si infringirá algún daño en este o a alguien que se encuentre en la parte trasera del vehículo. Existen variedad de cámaras entre las que se pueden destacar las convencionales, con intensificador de luz, con foco infrarrojos (IR) y térmicas.

Lo que sin duda es un avance sobre el desarrollo de sistemas de visión en vehículos es el radar Lidar, el que permite realizar un rastreo de toda la zona generando un mapeo de alta resolución que permite determinar las distancias exactas y posición de los objetos que se encuentran en cercanía del vehículo.

Experiencias de otros ejércitos

En lo que respecta a otros ejércitos se analizará la información existente sobre el Leopardo 2E, el Leopard 2A7+, los equipos con que fue dotado el M1 A1 Abrams, Leopard 2E can y la experiencia de uso de sistemas de realidad virtual del Ejército noruego.

- Ejército español

En el caso del Ejército de Tierra Español cabe destacar que su tanque principal de batalla (MBT) el Leopardo 2E, cuenta con tecnología incorporada de alta gama, posee una cámara delantera y una trasera que permiten al conductor tener la capacidad de discernir sobre los obstáculos en la parte delantera del tanque como en la parte posterior.

En la fotografía N° 1 se puede observar el tanque Leopardo 2E, con su sistema de apoyo al conductor basado en una cámara delantera y una cámara trasera. Además, se puede identificar la ubicación del monitor y su resolución.

Fotografía N° 1: Interior de Tanque Leopardo 2E.

Fuente: http://www.ejercitos.org/ngg_tag/carros-de-combate.

En la fotografía anteriormente presentada, se puede observar el sistema de la cámara instalada en la parte posterior del tanque Leopardo 2E, que le permite al conductor tener un ángulo de visión de la parte posterior del tanque Leopardo 2E. Se puede observar claramente el nivel de protección y sellado de su case.

A continuación se muestra en la Tabla N° 1 las características que poseen estas cámaras empleadas en el tanque Leopardo 2E.[5]

5 DIEZ DE DIEGO, Carlos (2018). Informe solicitud de antecedentes Leopardo 2E, España.

CARACTERÍSTICAS TÉCNICAS DEL SISTEMA DE APOYO AL CONDUCTOR ANTE MANIOBRAS EN REVERSA DEL LEOPARDO 2E	DESCRIPCIÓN
Tipo de Cámara	CCD-B/N, fotosensibilidad min.0,3 Lux distancia focal al objetivo 3,6 mm. Apertura del diafragma automática.
Sistema de intensificación de luz	Intensificador de Luz.
Ángulo de visión	Vertical 54° Horizontal 72°
Tipo de interfase	Alámbrica.
Ubicación del monitor	Lado izquierdo del puesto del conductor.
Costo aproximado	13.891,7 EUR
Sistema de protección o limpieza	Sistema de protección del lente y un sistema de cortinilla para limpieza de la lente.
Tipo de activación del sistema	Se activa solo a voluntad de conductor.
Lugar de alimentación eléctrica	Desde el panel en el cable U2
Lugar de paso de los cables	Por el costado del chasis en su parte interior por el lado izquierdo.
En qué actividades se emplea	Maniobras.

Tabla N° 1: Características técnicas Leopardo 2E.

Fuente: Elaboración propia.

- Ejército de EE.UU.

En el TARDEC,[6] EE.UU. se pudo obtener antecedentes sobre un sistema de advertencia de proximidad (SCMM) que tiene por función entregar al conductor y a la tripulación un mayor conocimiento situacional de los objetos que representan potenciales obstáculos cerca de la parte trasera del vehículo.[7]

El sistema usa sensores para detectar activamente objetos en la parte posterior del vehículo y medir el alcance. Se debe tener en cuenta en lo descrito por el TARDEC que el subsistema de advertencia de proximidad no detectará obstáculos negativos, por ejemplo, baches, zanjas, etc.

Cuando se detecta un objeto, el software del sistema SCMM enviará al subsistema de análisis la información de distancia del objeto para que la computadora de análisis la procese.

La tripulación, por su parte, recibe una notificación audible a través de sus intercomunicadores y visualmente en las pantallas de sus estaciones. Se debe tener en cuenta que la tripulación tiene la capacidad de habilitar y deshabilitar todas las notificaciones de proximidad. Sin

6 Centro de Investigación, Desarrollo e Ingeniería Automotriz de Tanques del Ejército de EE.UU.

7 BRIEF, Matt. Diseño del desarrollo de sistema de alerta de proximidad, elaborado por TARDEC, EE.UU., 1998.

embargo, la interfaz entre el software del sistema SCMM y el software de análisis no se verá afectada cuando la notificación de la tripulación esté desactivada.

Se debe considerar que el sistema antes descrito se encuentra en etapa de prototipo y, en el mismo sentido del presente trabajo, se puede analizar que los tanque M1 A2 Abrams del Ejército de EE.UU. y a los vehículos blindados, como el Bradley, les fueron incorporados sistemas de apoyo al conductor ante maniobras en reversa conformados por cámaras que se encuentran en un kit de instalación rápida, ya que se realiza el reemplazo del foco trasero derecho y se realiza la conexión con el monitor a través de cables.

Es un sistema de alta practicidad y aplicabilidad, ya que se adapta a toda la línea de vehículos del Ejército de EE.UU.

- Ejército alemán

El tanque Leopard 2A7+ alemán, cuenta con una cámara de retroceso elaborada por Carl Zeiss Optronics GMBH, denominada spectus. Este sistema es empleado en el Leopard 2A7+ tanto para la parte delantera como trasera.

El sistema de apoyo al conductor ante maniobras en reversa conformado por la cámara spectus, cuenta con las siguientes características técnicas especificadas en la siguiente tabla.[8]

CARACTERÍSTICAS TÉCNICAS	DETALLE
Estándar de protección MIL STD 810	Para temperatura, golpe y vibraciones y presión de aire.
Compatibilidad electromagnética	Según la norma VG 95373
Temperatura de funcionamiento	-32 a 63° C°
Peso	7 kg
Longitud de infrarrojo	8 a 14 um
Alcance de la cámara	400 a 700 metros
Intensificador de luz	400 a 900 metros
Campo de visión	51° X 38,25°

Tabla N° 2: Características técnicas de la cámara spectus.

Fuente: Elaboración propia.

- Ejército canadiense

En la participación del Ejército de Chile en el ejercicio Wortingthon Challenge (2016), donde tripulaciones nacionales concurrieron a Canadá y emplearon los tanques Leopard

8 Hendsoldt en línea, MÜLLER, Thomas, 2018, cámara spectus, disponible en www.hendsoldt.com, Alemania.

2 canadienses, los que cuentan con un sistema de apoyo al conductor ante maniobras en reversa, en específico el sistema se trata de una cámara, del que se obtuvieron los siguientes antecedentes a través de los conductores que participaron en dicho ejercicio militar.

Los conductores de nuestro Ejército detallan que este ejercicio se realizó en el tanque principal de batalla canadiense el Leopard 2A4 Can, el que cuenta con un sistema de apoyo al conductor ante maniobras en reversa. Además, destacan que el respaldo que entrega el poseer esta cámara es una real ayuda para el conductor y la tripulación, ya que el uso de este sistema, libera al comandante de tanque y al municionero, quienes pueden cumplir con sus funciones sin la necesidad de cooperar en los movimientos marcha atrás, ya que este sistema entrega al conductor una mayor seguridad en las maniobras en reversa y una mejor visión de la que puede tener el comandante y el conductor.

La descripción del sistema realizada por los conductores especifica que es una cámara ubicada en la parte trasera del tanque, conectada al volante de conducción, que tiene dos comandos, uno sirve para seleccionar la cámara a usar, el segundo es para la visión lateral izquierda, lateral derecha o central. La cámara está protegida por una caja metálica con vidrio, la pantalla está en el puesto del conductor y puede ser apagada a voluntad, teniendo incorporada guías para centrarse en el camino, finalmente, cabe señalar que se regula el brillo y contraste de la cámara.

- Ejército noruego

En la búsqueda de antecedentes de sistemas de apoyo a la conducción en reversa empleados en sistemas de armas, se menciona en variadas fuentes la experiencia del Ejército noruego empleando el sistema Oculus Rift[9] en la conducción de tanques.[10]

El sistema utiliza cámaras distribuidas alrededor de un vehículo de combate blindado, para obtener imágenes desde diferentes puntos de vista que son enviadas al ordenador que procesa el entorno virtual que es mostrado en tiempo real en las gafas de realidad virtual Oculus Rift.

Este sistema también cuenta con factores en contra, debido a que, en diferentes experiencias con la realidad virtual, se ha podido evidenciar que funciona perfecto hasta que se inicia el movimiento del vehículo, debido a que se produce una pérdida del sentido de orientación y mareos por parte de los usuarios lo que se denomina cinetosis, la que produce un riesgo elevado para el conductor y la tripulación de desorientarse.

9 Es un sistema conformado por un casco de realidad virtual y cámaras de 360°

10 *The Atlantic,* MOSENDZ, Polly, 2014. El ejército noruego está usando Oculus para conducir sus tanques, en línea, disponible en www.theatlantic.com, Noruega.

Sistemas de apoyo al conductor ante maniobras en reversa a nivel mundial

A nivel mundial podemos ver cómo se muestra una tendencia en cuanto a la incorporación de sistemas de apoyo al conductor ante maniobras en reversa, debido a que el 41% de los tanques de tercera, cuarta y quinta generación cuentan con sistemas de cámaras para ello.

Tanques a nivel mundial, con sistema de apoyo al conductor ante maniobras en reversa.

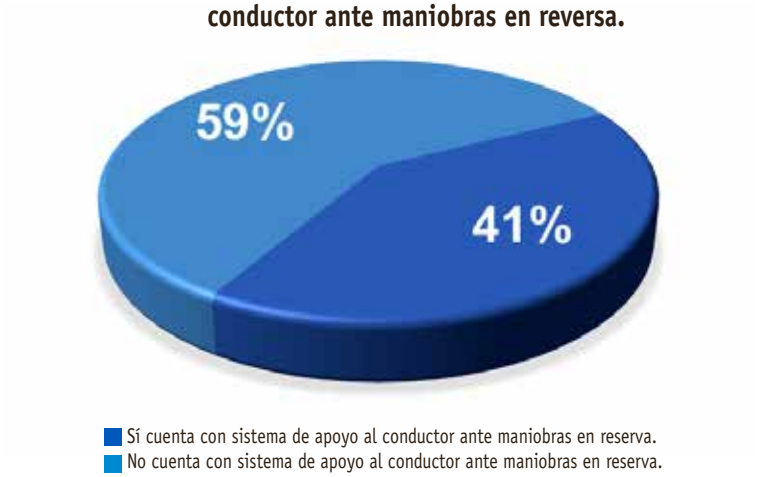


Gráfico N° 1: Porcentaje de sistemas de apoyo al conductor ante maniobras en reversa en el mundo.

Fuente: Elaboración propia.

Análisis realizado a cuestionarios enviados a los conductores de tanque Leopard 2A4

Se enviaron cuestionarios a los grupos blindados que cuentan con material Leopard 2A4 y al CECOMBAC,[11] los que se dirigían a los conductores.

Dentro de las respuestas entregadas en estos cuestionarios se pueden extraer las siguientes.

Los conductores que contestaron este cuestionario en formato enviado son 35, desempeñándose como conductores con un promedio de 4,4 años, lo que permite establecer que estamos frente a conductores que tienen en general un conocimiento avanzado del sistema de armas tanque Leopard 2A4.

Ante la pregunta según su punto de vista "¿Cree usted que el tanque Leopard 2A4 posee una buena visión de la parte posterior?", 29 de los 35 conductores, el 83% expresan que el tanque no

11 Centro de Entrenamiento de Combate Acorazado del Ejército de Chile.

tiene buena visión de la parte posterior y tan solo un 17% de los conductores dice que sí cuenta con una buena visión de la parte trasera, lo anterior es inferido refiriéndose al uso de guías según lo establece la doctrina.

En la pregunta número tres que se enfoca en saber si el conductor ha sufrido algún accidente en maniobras en reversa con el tanque Leopard 2A4, es claro destacar que tan solo 3 de los conductores, lo que representa un 9%, dice haber sufrido percances menores. Se debe tener en cuenta que, en esta pregunta, desde un comienzo, se planteó la dificultad que alguno de los conductores declarara algún accidente, por menor que este fuera, de hecho 29 conductores (91% del total) declara no haber sufrido ninguno.

En la pregunta número cuatro donde se plantea al conductor si es necesaria la instalación de un sistema de apoyo al conductor ante maniobras en reversa o basta con los procedimientos doctrinarios, 28 de los 35 conductores, el 80%, contestaron que sí se hace necesaria la instalación de un sistema de apoyo ante maniobras en reversa y tan solo 7 conductores que conforman un 20%, dice que no es necesaria la instalación de un sistema de apoyo ante maniobras en reversa, que tan solo basta con el procedimiento establecido en la doctrina.

En la pregunta número cinco, donde se muestran los sistemas existentes aplicables en un sistema de apoyo al conductor ante maniobras en reversa en el tanque Leopard 2A4 y se les solicita a los conductores escoger uno. 21 de los conductores, el 60%, cree que el mejor sistema para integrar al tanque Leopard 2A4 es una cámara; 3, el 9%, creen que lo mejor es un sistema de sensores de ultrasonido; 3 conductores, el 9%, creen que lo mejor es un sistema de radar Lidar; 2 conductores restantes, el 6%, creen que lo mejor es el sistema de sensores de cintas magnéticas y, finalmente, 6 conductores conformando un 17% no contestaron.

En la pregunta número seis, donde se plantea a los conductores en qué parte instalarían el sistema de apoyo al conductor ante maniobras en reversa, se destaca que 18, un 51%, coincidieron que debe ir en la parte trasera superior del tanque; 6 conductores, un 17%, creen que debe ir en la parte posterior del tanque al medio; 1 conductor, que conforma el 3%, cree que debe ir en la torre y los últimos 10 conductores, el 29%, no saben dónde colocar el sistema.

En la pregunta número siete, se pregunta a los conductores, según su experiencia ¿El sistema de apoyo al conductor ante maniobras en reversa del tanque Leopard 2A4, debe contar con un sistema que le permita operar en forma nocturna? 26 conductores, un 74%, consideran que si es necesario que este sistema cuente con la capacidad de operar en forma nocturna; tan solo 9 conductores, el 26%, no creen que sea necesaria la instalación de un sistema de visión nocturna.

En la pregunta número ocho, donde se realiza la pregunta a los conductores si creen que el sistema al conductor ante maniobras en reversa les servirá en maniobras en el box, 23 conductores,

un 66%, considera que sí sería útil el sistema de apoyo al conductor ante maniobras en reversa en el box, 12 conductores, un 34%, creen que este sistema no serviría en el box.

En la pregunta número nueve, donde se les pregunta a los conductores si creen que el sistema de apoyo ante maniobras en reversa les serviría para bajar el tanque Leopard 2A4 de la cama baja, 17 conductores, un 49%, creen que no servirá y 16 conductores, un 46%, creen que si servirá para apoyar en la carga y descarga del tanque Leopard 2A4 de una cama baja.

En la pregunta número diez donde se pregunta a los conductores si creen que el sistema de apoyo al conductor ante maniobras en reversa les serviría en el combate, 12 conductores, un 34%, creen que sí les serviría en combate y 20 conductores, un 57%, creen que no serviría en el combate y, finalmente, 3 conductores, un 9%, no contestaron.

En la pregunta número once, donde se plantea la pregunta en qué procedimiento o circunstancia creen los conductores que serviría el sistema de apoyo al conductor ante maniobras en reversa se destacan dentro de las respuestas las siguientes:

- Cambios de formaciones
- Cruces de campo minado
- Fuego retrógrado
- Ante ataque aéreo
- En el desprendimiento
- En un movimiento retrógrado
- En cambio, de formaciones
- Al buscar desenfilada de chasis retrocediendo
- Ocultamiento cuando se utiliza fumígeno
- Al tractar un tanque
- Para realizar maniobras de conducción en el box
- Para observar al conectar estrobos
- Para no vulnerar las medidas de seguridad

En la pregunta número doce, donde se plantea a los conductores que establezcan sus ideas o propuestas con respecto a este sistema se destaca:

- La preocupación respecto al ambiente con excesivo polvo
- La necesidad de que este sistema sea blindado
- Que el sistema se encuentra sellado antiagua

Principalmente, que el sistema pueda ser operado sin problema en la zona norte de nuestro país.

Como resultado de este cuestionario se realizó un análisis exhaustivo determinando ciertos requerimientos necesarios de incorporar al sistema de apoyo al conductor ante maniobras en reversa en el tanque Leopard 2A4.

PROPUESTA DE SISTEMA DE APOYO AL CONDUCTOR ANTE MANIOBRAS EN REVERSA

La propuesta para la integración de un sistema de apoyo al conductor ante maniobras en reversa, busca el dar solución a todos los requerimientos planteados por:

- Conductores
- Miembros de la tripulación
- Instructores
- Mantenedores del tanque Leopard 2A4

Para ello se plantea el modelo físico de un demostrador tecnológico el que se basa en el siguiente diagrama:

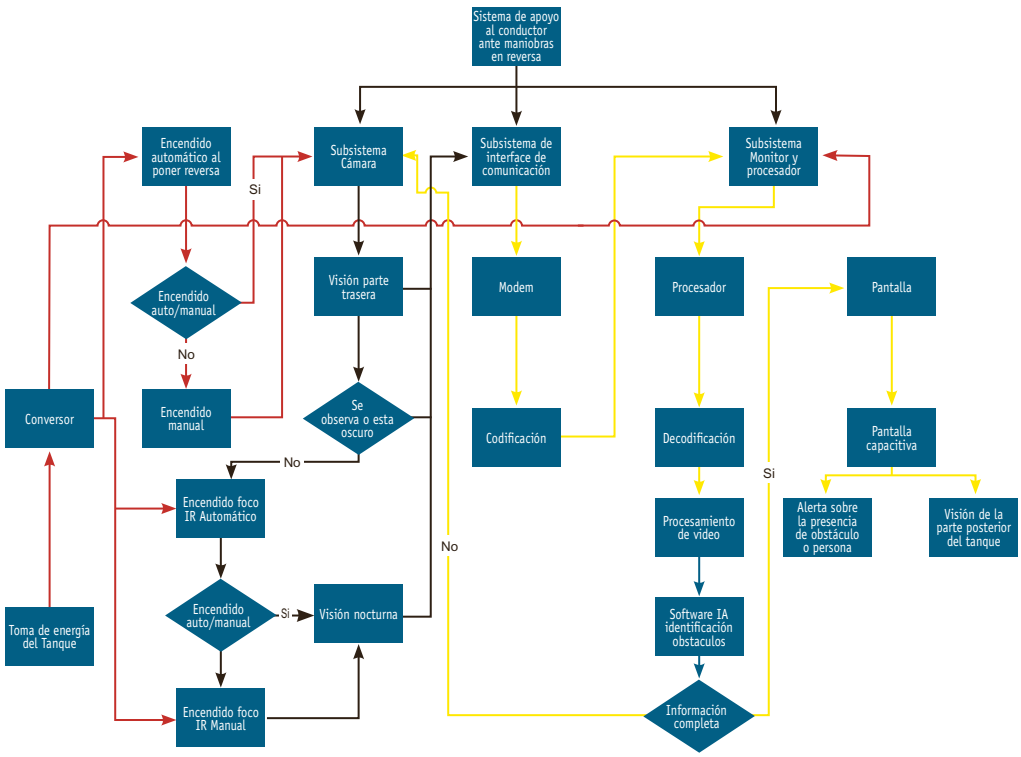


Figura N° 1: Diagrama del demostrador tecnológico.

Fuente: Elaboración propia.

En la (Figura N°1) en la que se muestra el diagrama del demostrador tecnológico, el que nos permite apreciar los subsistemas y sus interfaces. Se iniciará describiendo la energía eléctrica la que será extraída a modo experimental de los sistemas de conexión de la lámpara del tanque Leopard 2A4. Posteriormente, esta energía será conducida a un conversor que la transformará de 24v DC a 220v AC, para luego pasar a la caja de conexión en la que se ubicarán los trasformadores de la cámara y del procesador, en general las cámaras en el mercado operan con 9v AC y los procesadores con 19 v AC.

Existe la capacidad de activar el sistema en forma automática al seleccionar la reversa, ya que esta permitirá sin retardo, poder apreciar los posibles obstáculos existentes en la parte posterior del tanque, también se optó por la instalación de un sistema de activación manual, ya que este permitirá tener visual de la parte posterior a voluntad del conductor.

La cámara contará con una conexión directa al procesador permitiendo la transmisión bidireccional por esta, generando un flujo redundante de información, lo que entrega una mayor confiabilidad en la operación del sistema.

Existe la capacidad de encender en forma automática el foco infrarrojo (IR) y en forma manual, ya que este foco de no tener sistema manual por configuración general de los sistemas de cámaras disponibles en el mercado se activará automáticamente siendo esta contrario a las medidas de protección electrónica.

El software de inteligencia artificial tendrá redundancia, debido a que este podría quedar con datos incompletos y debe concurrir a emplear más informaciones en caso de ser necesario.

En la integración de una cámara de características básicas de compatibilidad electromagnética, protección IP 64[12] como mínimo y de fácil adquisición e instalación. También se aplica el uso de una cámara CCD,[13] debido al alto costo de una cámara térmica, pero esta cámara debe contar con una capacidad de visión de 50 metros con el sistema de foco IR encendido y, además, debe poseer un ángulo de visión de más de 90°.

En cuanto al monitor planteado se necesita la instalación de un sistema de pantalla de características similares a la cámara. A su vez, en esta investigación se optó por la integración de un computador de panel, evitando el uso del sistema Arduino o Raspberry por la baja confiabilidad de este tipo de procesadores en tareas con softwares de alta gama, para así poder realizar análisis en

12 IP Ingress Protection, Norma internacional IEC 60528 Degrees of Protection, IP 64, Protección completa contra contacto, protección contra penetración de polvo, protegido contra la penetración de agua en caso de invasión pasajera.

13 CCD (Charge Coupled Device o, en español, Dispositivo de Carga Acoplada). Este tipo de sensor lo tienen la mayoría de las cámaras digitales.

cuanto a la integración de otras capacidades asociadas a este sistema como inteligencia artificial y otros sistemas de detección basados en software.

En cuanto al sistema de conexión eléctrico en esta investigación, se optó por la integración de un conversor de 24V a los equipos implementados para así poder realizar pruebas en seco y no incurrir en trabajos que requieren el intervenir el vehículo.

En cuanto a los case, estos se desarrollaron en acero y buscan el poder integrarse en los puntos de anclaje ya existentes en el tanque para así poder realizar pruebas sin intervenir el vehículo.

Referente a los cables, en el demostrador tecnológico desarrollado, estos se montaron para la realización de pruebas por el exterior, pero es completamente factible la integración, estas en conjunto con el sistema eléctrico del vehículo.

Una vez realizado este análisis se procedió a la adquisición de los componentes y se realizó la confección del siguiente modelo en la figura N° 2 en la que se pueden observar los componentes y sus respectivas interfaces.

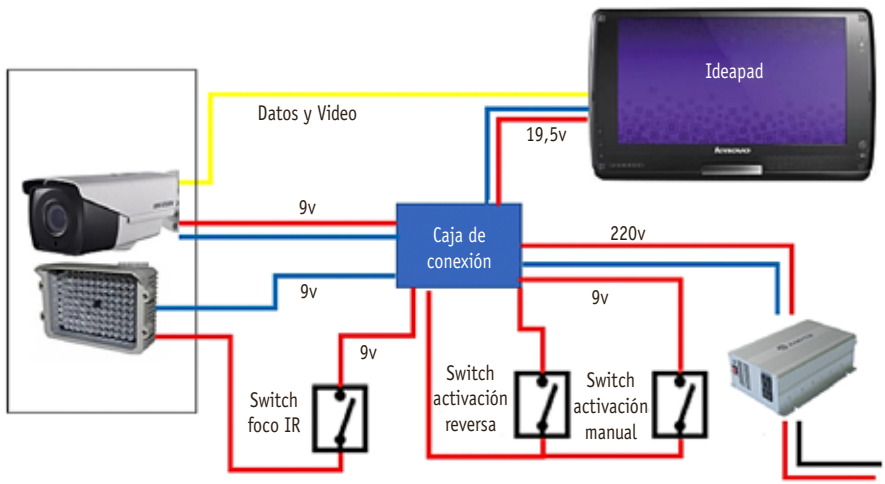


Figura N° 2: Modelo del demostrador tecnológico desarrollado.

Fuente: Elaboración propia.

Se realizaron las primeras pruebas entregando los resultados esperados en cuanto a la integración de un ángulo de visión de la parte posterior del tanque, entregando al conductor claramente una visión de la parte posterior se hace necesario el implementar completamente los case, para así realizar pruebas de anclaje del sistema al vehículo y poder efectuar pruebas en terreno.

Fotografía N° 2: Pruebas iniciales realizadas al demostrador tecnológico.

Fuente: Elaboración propia.

En la fotografía se muestra el demostrador tecnológico del sistema de apoyo al conductor ante maniobras en reversa siendo probado en el tanque Leopard 2A4, dentro del box con respecto al funcionamiento general y capacidad de identificación de objetos que representan posibles obstáculos para el vehículo.

CONCLUSIONES

A través de lo investigado a nivel internacional y lo expuesto en este artículo, se puede determinar que es totalmente factible la integración al tanque Leopard 2A4 de sistemas de sensores electrónicos que le permitan aumentar más sus prestaciones logrando así, mantener el nivel de seguridad en la operación del tanque Leopard 2A4 en cuanto a los movimientos en reversa.

En cuanto a la propuesta de incorporación de un sistema de apoyo al conductor ante maniobras en reversa se puede concluir que puede ser elaborado en nuestro país con nuestra tecnología, ya que este busca no interferir con los sistemas ya existentes en el tanque.

Lo importante de destacar es que el sistema propuesto representa un demostrador tecnológico que permite verificar la factibilidad del sistema y detalles de integración al tanque Leopard 2A4, después de realizar pruebas en todos los sistemas y al pasar al desarrollo en sí, se deberá realizar el análisis de integración al sistema, por ejemplo, de una cámara térmica.

Se realizaron pruebas en cuanto a la operación dentro del box del sistema sin aun integrar a la fecha las protecciones o case respectivos que permitan realizar pruebas en terreno y el estudiar la factibilidad de empleo de este sistema en procedimientos de combate del tanque Leopard 2A4.

BIBLIOGRAFÍA

BRIEF, Matt. Diseño del desarrollo de sistema de alerta de proximidad, elaborado por TARDEC, EE.UU.,1998.

DIEZ DE DIEGO, Carlos (2018). Informe solicitud de antecedentes Leopardo 2E, España.

MOSENDZ, Polly. *The Atlantic,* 2014. El ejército noruego está usando Oculus para conducir sus tanques, en línea, disponible en www.theatlantic.com, Noruega.

MÜLLER, Thomas. Hendsoldt en línea, 2018, cámara spectus, disponible en www.hendsoldt.com, Alemania.

PHILIPS, Malcom. "Main Battle tank Update", *Military Technology,* junio 2012.

ROJKES, Ami. Israel defense (en línea), 2016, El Trophy Rafael y el IronFist de IMI están en el blanco, disponible en www.israeldefense.com, Israel.

RECURSOS HUMANOS Y ESTUDIOS SOCIALES

MEMORIAL
DEL
Ejército de Chile

PRIMERA DETECCIÓN DE CRYPTOSPORIDIUM SPP., PARÁSITO INTESTINAL, EN MARISCOS DESTINADOS A CONSUMO HUMANO EN CHILE[1]

PAC JUAN QUIROGA SEPÚLVEDA[2]

Resumen: *el Servicio de Veterinaria conforme a las misiones asignadas en el área de salud ambiental, debe velar por la inocuidad y seguridad de los alimentos ofrecidos al interior de todas las instalaciones militares. En este contexto, este artículo[3] tiene como propósito, transferir los resultados de una investigación científica en desarrollo realizada en materias de seguridad alimentaria, en donde se realizó por primera vez en el país, la detección microscópica del parásito intestinal, Cryptosporidium spp., en mariscos destinados a consumo humano, aportando así, a la epidemiología de agentes microbiológicos que producen enfermedad de transmisión alimentaria.*
Palabras clave: *parásito, marisco, alimento, epidemiología, Cryptosporidium spp.*

Abstract: *the Veterinary Service, in accordance with the assigned missions in the area of environmental health, must ensure the safety and security of the food offered inside all military installations. In this context, this article aims to transfer results of a scientific research in development carried out in matters of food safety to this Service, that was performed for the first time in the country, the microscopic detection of the intestinal parasite, Cryptosporidium spp., in seafood destined for human consumption, this contributing to the epidemiology of microbiological agents that produce Food Transmission Diseases.*
Keywords: *parasite, shellfish, food, epidemiology, Cryptosporidium spp.*

---

1 Artículo ganador del primer puesto del concurso "Desarrollando Capacidades Militares", en el ámbito de Recursos Humanos y Estudios Sociales.

2 Médico Veterinario y Licenciado en Ciencias Veterinarias por la Universidad de Concepción. Magíster en Ciencias Animales y Veterinarias con mención en Medicina Preventiva Animal por la U. de Chile y Magíster en Dirección y Gestión de Personas por la U. Finis Terrae. Actualmente es candidato a Doctor por el Instituto de Nutrición y Tecnología de los Alimentos (INTA) de la Universidad de Chile.

3 Extracto de la investigación científica realizada por el autor, para optar al Grado de Doctor por el Instituto de Nutrición Tecnología de los Alimentos (INTA) de la Universidad de Chile.

INTRODUCCIÓN

La alimentación como apoyo de sostén a la fuerza terrestre

Las acciones destinadas a obtener, abastecer, mantener, transportar y atender a las tropas, cobran una especial relevancia en la generación de las condiciones necesarias para permitir y asegurar la operacionalidad de la fuerza.

Es en este orden de ideas, donde los componentes de la estructura de la fuerza, a los cuales deben estar destinados todos los recursos disponibles para asegurar la capacidad combativa, constituyen al hombre como el mayor aspecto a considerar. Al ser entonces el capital humano el eje central de interés al que debe propender la institución, por ser quienes dan vida a la organización transformando el concepto de fuerza en algo tangible, es de suma relevancia, que todo el personal se encuentre abastecido de una alimentación adecuada para recuperar la fuerza, mantener la salud y obtener las energías necesarias para enfrentar los desafíos del día a día.[4]

Antiguamente, se creía que la alimentación era solo esencial para la supervivencia y la satisfacción del hambre, sin embargo hoy impera el concepto de una alimentación saludable, equilibrada e inocua (que no produce daño), dando mayor relevancia a este último concepto.[5]

Hoy, la Organización Mundial de la Salud (OMS) define la inocuidad de los alimentos como: *"toda acción encaminada para garantizar la máxima seguridad posible de los alimentos, abarcando toda la cadena alimenticia, desde la producción hasta el consumo".*[6] Construyéndose en la actualidad, una gran vinculación entre la moral, el desempeño y lo que se come, quedando de manifiesto el importante rol que cumple la alimentación en los soldados, siendo considerada como una de las acciones más destacadas al interior de la institución.[7]

El Servicio de Veterinaria en la protección de la inocuidad y seguridad alimentaria al interior del Ejército

Al interior de la organización militar, para que pueda cumplir con la responsabilidad global de su tropa en materias de higiene ambiental, el comandante posee la importante asesoría de profesionales adiestrados para ello. Para dar cumplimiento a este deber, el comandante posee el apoyo de profesionales del Servicio de Veterinaria del Ejército, que junto con la colaboración de otros entendidos, tales como médicos, odontólogos, enfermeros, entre otros,

4 EJÉRCITO DE CHILE, Manual de Cocina Militar, División Logística, Santiago, Chile, 2008, p. 5.
5 *Ibídem*, p. 6.
6 Disponible en: http://www.who.int/topics/food_safety/es/
7 EJÉRCITO DE CHILE, Manual..., *op.cit.*, p. 5.

lo deben asesorar para, finalmente, dar el correcto cumplimiento a la protección sanitaria global de su personal.[8]

Ya lo decía hace casi 60 años atrás, el teniente coronel Teodoro Poseck, oficial de Veterinaria, durante el "Foro de Alimentación del Ejército" realizado el 15 y 16 de diciembre de 1959 en el Auditorio del Estado Mayor, donde expuso que: *"la participación del Servicio de Veterinaria en la higiene de los alimentos, tiene claros objetivos por alcanzar y además, debe tener las atribuciones en cuanto a la obtención de la principal de esas funciones, que es, desde luego, la de proteger la salud del personal militar de las enfermedades vehiculizadas por intermedio de los alimentos de origen animal".* Quedando finalmente bajo acta, que: *"la inspección de los alimentos de cualquier origen para el consumo humano institucional, debía ser efectuado por el Servicio de Veterinaria del Ejército".*[9]

El Servicio de Veterinaria del Ejército de Chile, hoy en día, conforme a la misión que se le asigna en el área de salud ambiental,[10] establece el Sistema de Salud Ambiental del Ejército, el que tiene por misión dar satisfacción a todos los requerimientos que en este ámbito se generan en la institución.

Este servicio debe ejecutar el Programa de "Inocuidad Alimentaria y del Agua", cuyo objetivo principal es disminuir los riesgos de enfermedades que puedan afectar la salud del personal, asociadas al peligro de consumir alimentos y agua contaminados con agentes microbiológicos o fisicoquímicos.[11] Por ello, se hace prioritario el mantener una permanente actualización de conocimientos referidos a materias de inocuidad alimentaria por parte del personal del Servicio,[12] más aún en patógenos alimentarios emergentes, descubiertos tanto en Chile como en el mundo en los diferentes grupos alimentarios, contribuyendo de esta manera a la correcta comunicación e intercambio de información entre las entidades gubernamentales de salud (SEREMIS[13] de Salud), y las institucionales (ASE[14]) del Ejército de Chile.

CRIPTOSPORIDIOSIS

La enfermedad causada por protozoos del género Cryptosporidium, tanto en animales como seres humanos se denomina Criptosporidiosis. Corresponde a una enfermedad parasitaria de importancia

8 EJÉRCITO DE CHILE, Manual de Higiene Ambiental y Control de Alimentos, Comando de Apoyo Logístico, Santiago, Chile, 1987, p. 7.
9 EJÉRCITO DE CHILE, Foro de Alimentación: Los problemas alimentarios del Ejercito, Dirección de Sanidad Militar, Santiago, 1960, pp. 56, 58, 59, 70.
10 Conforme a la Orden de Comando CJE CGP DSE (R) N° 6030/1331 de 12.FEB.2016.
11 EJÉRCITO DE CHILE, Plan de Salud Ambiental 2016-2020, Comando General de Personal, Dirección de Sanidad, Santiago, 2016, pp. 3-4.
12 *Ibídem*, p. 36.
13 SEREMIS: Secretarias Regionales Ministeriales.
14 ASE: Autoridad Sanitaria del Ejército.

clínica en medicina y veterinaria, en donde el cuadro clínico en seres humanos, se caracteriza por una diarrea, que puede ser profusa y acuosa, acompañada de dolor abdominal, pérdida de apetito, náuseas y vómito.[15]

Mecanismo de transmisión

La transmisión en seres humanos es principalmente mediante la ingesta de agua y/o alimentos contaminados con este agente protozoario.[16] Esta vía indirecta, es la más significativa desde el punto de vista epidemiológico, en base a la diseminación de este agente, ya que posee ooquistes de pequeño tamaño, una gruesa pared ooquística, resistencia al tratamiento con cloro y ácidos, viabilidad prolongada de hasta varios meses en el ambiente, excreción de estadio inmediatamente inféctico (ooquiste), baja dosis infectante para infectar otros organismos (basta con la ingesta de un solo ooquiste) y considerable potencial zoonótico (transmitido desde los animales al hombre).[17]

Morfología

El ooquiste, que es el estadio infectivo, posee una alta resistencia al medio ambiente. Presenta una gruesa pared de forma esférica con un tamaño aproximado según la especie de 3 a 8,5 µm de diámetro.[18] Estos pueden ser eliminados en grandes cantidades por las heces y tienen la capacidad de sobrevivir por largos periodos de tiempo en aguas marinas, manteniéndose viables por hasta seis meses.[19]

Criptosporidiosis como enfermedad de transmisión alimentaria (ETA) y Enfermedad de notificación obligatoria (ENO) en Chile

La Criptosporidiosis humana es considerada una enfermedad de transmisión alimentaria (ETA), cuando es transmitida por la ingestión de alimentos y/o agua contaminada con Cryptosporidium. Esta enfermedad, al ser diagnosticada en forma de brote (dos o más personas infectadas), ingresa al listado de enfermedades de notificación obligatoria (ENO), teniendo el carácter de notificación inmediata por el Decreto Supremo N° 158/2004 del Ministerio de Salud,[20] por lo que tiene una vigilancia epidemiológica especial a las demás patologías gastrointestinales en el país.

---

15 ORGANIZACION MUNDIAL DE LA SALUD, El control de las enfermedades transmisibles, Washington, EE.UU., 2001, p. 94.

16 GÓMEZ-CUOSO, H., *et al.,* Cryptosporidium contamination in harvest areas of bivalve molluscs, *Journal of Food Protection,* 69: 185–190, 2006.

17 MOLINA, R. *et al.,* Importancia de la detección del protozoario zoonótico Cryptosporidium parvum en muestras de agua. Avances en Ciencias Veterinarias, 25(1): 68-82, 2010.

18 FAYER, R. & XIAO, L. (2008). *Cryptosporidium and cryptosporidiosis.* Boca Ratón, Florida, E.E.U.U., CRC Press., p. 560.

19 DEL COCO, V. *et al.* Criptosporidiosis: una zoonosis emergente, *Revista Argentina de Microbiología,* 41(3): 185-196, 2009.

20 MINISTERIO DE SALUD, Reglamento sobre Notificación de Enfermedades Transmisibles de Declaración Obligatoria (ENO), DS N° 158/04, Publicado en el *Diario Oficial* de 10.05.05, Santiago, Chile.

Los estudios epidemiológicos de ETA en el país, durante el período 2017, determinaron que el principal alimento sospechoso involucrado en los brotes de este tipo de enfermedades, fue el molusco bivalvo fresco (marisco),[21] dados principalmente por la gran capacidad de retención de elementos físicos, químicos y biológicos de tipo contaminante y potencialmente patógenos presentes en las aguas marinas.

Detección de Cryptosporidium spp. en mariscos destinados a consumo humano

En ambientes marinos, Cryptosporidium spp. se encuentra principalmente en áreas que se ven afectadas por el desbordamiento de aguas residuales hacia el mar, o en aguas que aumentaron su escurrimiento, tanto a nivel urbano como agrícola, principalmente por las lluvias, arrastrando el parásito a las costas, ocasionando contaminación medioambiental.[22]

Es por ello que, estudios realizados durante las últimas dos décadas alrededor del globo, utilizando diferentes métodos de detección, han permitido establecer la presencia de ooquistes de Cryptosporidium spp. en el interior de mariscos destinados a consumo humano, los cuales bioacumulan el parásito gastrointestinal en su interior, debido a que estos filtran pequeñas partículas provenientes del agua para su alimentación.[23, 24, 25]

Inactivación de los ooquistes de Cryptosporidium spp. en mariscos

Se ha descubierto que el marisco debe ser sometido a una temperatura de cocción sobre los 65 ºC durante más de dos minutos, para inactivar el ooquiste de Cryptosporidium spp.[26] Esto se debe a la composición proteica de la pared ooquística, la que es desnaturalizada a temperatura elevada.[27]

De igual forma, temperaturas de congelación alteran la infectividad ooquística de Cryptosporidium spp., sin embargo únicamente a temperaturas por bajo de los -70 °C, se ha demostrado que se inactiva el ooquiste de Cryptosporidium spp.[28]

---

21 Disponible en: http://www.deis.cl/wp-content/2017/gobCL-sitios-1.0/assets/BroteETA.html

22 GOMEZ-CUOSO, H. *et al.*, Cryptosporidium… (2006), *op.cit.*, pp. 185-190.

23 FREIRE-SANTOS, F. *et al.*, Detection of Cryptosporidium oocysts in bivalve mollusks destined for human consumption, *Journal of Parasitology,* 86:853-854, 2000.

24 GIANGASPERO, A. *et al.*, Cryptosporidium parvum oocysts in seawater clams (Chamelea gallina) in Italy. Preventive Veterinary Medicine, 69: 203-212, 2005.

25 GOMEZ-BAUTISTA, M., *et al.*, Detection of infectious Cryptosporidium parvum oocysts in mussels (Mytilus galloprovincialis) and cockles (Cerastoderma edule). Applied and Environmental Microbiology, 66: 1866-1870, 2000.

26 FAYER, R., Effect of high temperature on infectivity of Cryptosporidium parvum oocysts in water, Applied and Environmental Microbiology, 60(8): 2732-2735, 1994.

27 GOMEZ-CUOSO, H. Cryptosporidium en moluscos bivalvos, Tesis PhD, Universidad de Santiago de Compostela, Santiago de Compostela, España, 2006, p. 187.

28 FAYER, R. *et al.*, Infectivity of Cryptosporidium parvum oocysts stored in water atenvironmental temperatures, *Journal of Parasitology,* 84:1165–1169, 1998.

Detección de Cryptosporidium spp. en Chile

La investigación científica nacional desarrollada en torno a la detección de Cryptosporidium spp. es extremadamente escasa. Los métodos de diagnóstico utilizados han sido la detección microscópica y molecular, realizando detección en seres humanos,[29] primates no humanos,[30] caninos,[31] bovinos,[32] ovinos,[33] caprinos,[34] equinos,[35] aves marinas[36] y en gastrópodos silvestres.[37] Hasta la fecha, no se ha realizado la detección microscópica de Cryptosporidium spp. en mariscos destinados a consumo humano en el país, siendo este, el principal alimento sospechoso involucrado en los brotes de ETA notificados al Ministerio de Salud.[38]

De los mariscos cultivados en Chile, es el chorito *(M. chilensis)*, el que posee el mayor consumo per cápita, siendo consumido en fresco y congelado, mientras que para el mercado internacional es exportado en formato cocido, fresco-enfriado, congelado, ahumado y en conserva.[39]

El objetivo principal de esta investigación, fue determinar y demostrar científicamente si existe la presencia de la forma infecciosa –ooquiste– de Cryptosporidium spp. al interior de mariscos *(M. chilensis)* destinados a consumo humano de centros de cultivo de la Región de Los Lagos, Chile, lo que posibilitaría la adopción de medidas institucionales y su difusión a nivel nacional.

DESARROLLO

Selección, tamaño y recolección de las muestras

Se fueron a recolectar choritos vivos *(Mytilus chilensis)*, provenientes de tres centros de cultivo comercial de la Región de Los Lagos.

---

29 PRADO, V. *et al.*, Enteritis por Cryptosporidium en un paciente leucémico, *Revista Chilena de Pediatría,* 56(4): 251-253, 1985.

30 BARRIOS, N.S., Estudio coproparasitario en primates no humanos del Parque Zoológico de Quilpué, V Región, Chile, Tesis pregrado, Universidad Austral de Chile, Valdivia, Chile, 2005, p. 30.

31 GORMAN, T. *et al.*, Parasitismo gastrointestinal en perros de comunas de Santiago de diferente nivel socioeconómico, *Revista de Parasitología Latinoamericana,* 61: 126-132, 2006.

32 DÍAZ-LEE, A. *et al.*, Analytical sensitivity of staining and molecular techniques for the detection of Cryptosporidium spp. oocysts isolated from bovines in water samples: a preliminary study, Archivos de Medicina Veterinaria, 47: 91-96, 2015.

33 TEXIA, G. *et al.* Criptosporidiosis en ovinos y caprinos de la zona central de Chile. Archivos de Medicina Veterinaria, 22(2): 155-158, 1990.

34 *Ibídem*, pp. 155-158.

35 GORMAN, T. & GODOY, A. Hallazgo de Cryptosporidium spp. en un equino F. S. Inglés diarreico, *Monografías de Medicina Veterinaria,* 11(2): 11-15. 1989.

36 ARREDONDO, C.E., Detección de Cryptosporidium spp. en el Pingüino de Magallanes *(Spheniscus magellanicus)* en dos pingüineras de la Región de Magallanes y Antártica Chilena, Tesis Pregrado, Universidad de Chile, Santiago, Chile, 2014, p. 34.

37 NEIRA, P. *et al.*, Cryptosporidium parvum en gastrópodos silvestres como bioindicadores de contaminación fecal en ecosistemas terrestres, *Revista Chilena de Infectología*, 27(3): 211-218, 2010.

38 Disponible en: http://www.deis.cl/wp-content/2017/gobCL-sitios-1.0/assets/BroteETA.html

39 ARANA. P. (2012). *Recursos Pesqueros del Mar de Chile.* Valparaíso, Chile. Editorial Universitaria de Valparaíso.

Los centros de cultivo están ubicados en Calbuco (41°46'00"S, 73°08'00"0), Castro (42°30'S, 74°00"0) y Quellón (43°06'S, 73°36"0), realizando cuatro muestreos estacionales, durante los meses de junio de 2017 (otoño), septiembre de 2017 (invierno), diciembre de 2017 (primavera) y marzo de 2018 (verano), en los respectivos centros de cultivo.

En las áreas definidas de cada centro, se seleccionaron dos cuelgas, extrayendo 20 ejemplares a 1 m de profundidad en cada una de ellas, obteniendo un total de 40 ejemplares por centro de cultivo.

De esta manera, se obtuvo un total por muestreo estacional de 120 muestras. Al final de este estudio, se obtuvo un total de 480 ejemplares de mariscos adultos, los cuales fueron analizados posteriormente en laboratorio.

CENTRO DE CULTIVO/ LOCALIDAD	CUELGA	OTOÑO	INVIERNO	PRIMAVERA	VERANO	TOTAL
Centro N° 1/ Calbuco	1	20	20	20	20	**80**
	2	20	20	20	20	**80**
Centro N° 2/ Castro	1	20	20	20	20	**80**
	2	20	20	20	20	**80**
Centro N° 3 / Quellón	1	20	20	20	20	**80**
	2	20	20	20	20	**80**
	TOTAL	**120**	**120**	**120**	**120**	**480**

Tabla N° 1: Diseño del muestreo aleatorio estacional de recolección de mariscos (M. chilensis), desde centros de cultivo de la Región de Los lagos, Chile.

Fuente. Elaboración propia.

Procesamiento inicial de las muestras

El procesamiento inicial de las muestras fue realizado en el Laboratorio del Centro Acuícola y Pesquero de Investigación Aplicada (CAPIA) de la Universidad Santo Tomás en la sede de Puerto Montt.

Se realizó un corte en diagonal en cada ejemplar obteniendo una "lonja", que se incorporó a un histocassette, procedimiento descrito en la Fig. N° 1 (desde la letra A a la F), los cuales quedaron almacenados en un fijador de mantenimiento de muestra, para ser enviados posteriormente al Laboratorio de Histología de la Universidad Católica del Norte en la ciudad de Coquimbo, IV Región, para realizar la generación de las placas histológicas, el corte, la tinción y la detección microscópica de Cryptosporidium spp.

Generación de placas histológicas

Los histocassettes con los tejidos fueron deshidratados, aclarados y preincluidos en un procesador automático durante la noche.

Posteriormente, se abrió cada histocassette, para disponer el tejido en un molde de acero inoxidable, el cual se llenó de parafina líquida (paraplast), hasta dejar enfriar en el centro de inclusión.

Una vez enfriado, el bloque se raspó en los costados y quedó listo para ser cortado. Procedimiento descrito en la Fig. N° 1 (desde la letra G a la M).

A) Medición de la concha.
B) Corte entre el pie (P) y el biso (B).
C) Mitad anterior y posterior del ejemplar.
D) Corte de la "lonja" en diagonal.
E) Cara de la lonja incorporada al histocassette con las estructuras de interés.
F) Histocassette marcado con lápiz de mina.
G) Apertura del histocassette.
H) Incorporación del tejido de la muestra en molde de acero inoxidable.
I) Incorporación de parafina líquida al tejido.
J) Molde de parafina con tejido en frío, retirado del molde de acero.
K) Raspado de bordes del bloque parafinado en frío con el tejido en su interior.
L) Bloque parafinado en frío con el tejido.
M) Centro de inclusión Thermo-Shandon, en donde se realiza el procedimiento de confección del bloque parafinado con tejido para realizar posteriormente el corte histológico.

Figura N° 1: Pasos para la obtención de la "lonja" por ejemplar (letra A a la F), y pasos para la obtención del bloque parafinado para muestra histológica (letra G a la M).

Fuente: Fotografías del autor.

Corte y tinción para la detección microscópica de Cryptosporidium spp.

Los bloques fueron cortados a un grosor de 5 µm, en un micrótomo manual de rotación (Fig. 2-A), siendo depositados en un baño termorregulado con albúmina (Fig. 2-B). Una vez estirados, se recogieron con el portaobjetos y se pusieron a secar en una estufa de laboratorio (Fig. 2-C), entre los 45-50 °C. El corte se pegó al vidrio con ayuda de la albúmina, dejando al menos una noche que se secara. Se realizó un corte por cada bloque, el que fue teñido con la técnica de Ziehl Neelsen (ZN), para la detección de Cryptosporidium spp., tinción específica para la detección de este microorganismo.[40]

Figura N° 2: Equipamiento de laboratorio, para realizar el corte histológico del bloque parafinado y tinción final para la detección de Cryptosporidium spp. en tejidos del marisco.

Fuente: Fotografías del autor.

A) Micrótomo manual de rotación.
B) Baño termorregulado o Baño María para secciones histológicas.

40 FAYER, R. & XIAO, L. (2008). Cryptosporidium... , *op.cit.*, p. 560.

C) Estufa de laboratorio.
D) Gabinete de bioseguridad tipo II con la batería de xiloles, etanoles y tinción Zielh Neelsen modificado en su interior, para realizar la detección de Cryptosporidium spp.

Para realizar la tinción, los cortes se colocaron en canastillos de tinción, ubicados en un gabinete de bioseguridad (Fig. 2-D), pasando por una batería de varios xiloles y varios etanoles decrecientes, hasta agua destilada, en donde, a partir de esta etapa, se realizaron las tinciones. Después de la tinción se realizó el proceso inverso en otra batería: deshidratación, aclarado y finalmente el montaje con medio de montaje de secado rápido Thermo-Shandon. Al día siguiente se limpiaron las placas del exceso de medio de montaje y se etiquetaron.

Una muestra se consideró positiva a Cryptosporidium spp. si al examen microscópico directo se realizaba la detección de, al menos, un ooquiste que cumpliera con los criterios de propiedades ópticas (color fucsia), tamaño (3 a 8 µm) y forma (esférico u oval) descritas en la literatura especializada.[41]

Hallazgos en las placas histológicas

El análisis de las placas histológicas se realizó en un microscopio marca Zeiss modelo Axiostar con cámara fotográfica conectada al computador.

La información se registró directamente al computador en planilla Excel® con el número de la muestra, centro de cultivo, estación del muestreo, presencia o ausencia de ooquistes de Cryptosporidium spp. y cantidad de ooquistes por muestra en los casos de detección.

Descriptores epidemiológicos para cada población muestreada por localidad y estación del año

Con los resultados obtenidos, se determinó la prevalencia de Cryptosporidium spp. (porcentaje de individuos que presentan ooquistes, independientemente de cuántos se detecten en la placa histológica), intensidad media (suma del total de ooquistes dividido solo por el número de ejemplares parasitados), rango de intensidad (la cantidad mínima y máxima de ooquistes detectados) y abundancia media (suma del total de ooquistes dividido por el total de ejemplares muestreados).[42]

41 *Ibídem*.
42 BUSH, A. *et al.*, Parasitology Meets Ecology on Its Own Terms: Margolis *et al.* revisited. J. Parasitol., 83(4): 575-583, 1997.

RESULTADOS

CENTRO DE CULTIVO/ LOCALIDAD	OTOÑO 2017				
	n	Prevalencia (%)	Intensidad media	Rango de intensidad	Abundancia media
Centro N° 1 - Calbuco	40	12,5	(13/5) = 2,6	1 a 5	(13/40) = 0,3
Centro N° 2 - Castro	40	45,0	(36/18) = 2,0	1 a 6	(36/40) = 0,9
Centro N° 3 - Quellón	40	27,5	(26/11) = 2,4	1 a 6	(26/40) = 0,7
INVIERNO 2017					
Centro N° 1 - Calbuco	40	62,5	(66/25) = 2,6	1 a 7	(66/40) = 1,7
Centro N° 2 - Castro	40	65,0	(65/26) = 2,5	1 a 14	(65/40) = 1,6
Centro N° 3 - Quellón	40	67,5	(67/27) = 2,5	1 a 6	(67/40) = 1,7
PRIMAVERA 2017					
Centro N° 1 - Calbuco	40	12,5	(10/5) = 2,0	1 a 4	(10/40) = 0,3
Centro N° 2 - Castro	40	2,5	(1/1) = 1,0	1	(1/40) = 0
Centro N° 3 - Quellón	40	10,0	(6/4) = 1,5	1 a 3	(6/40) = 0,2
VERANO 2018					
Centro N° 1 - Calbuco	40	12,5	(3/5) = 2,0	1 a 2	(3/40) = 0,07
Centro N° 2 - Castro	40	20,0	(1/1) = 1,0	1	(1/40) = 0,02
Centro N° 3 - Quellón	40	12,5	(6/3) = 1,5	1 a 2	(6/40) = 0,2

Tabla N° 2: Determinación de prevalencia, intensidad y abundancia media, y rango de intensidad de Cryptosporidium spp. detectados en chorito (M. chilensis) de la Región de Los Lagos, Chile, durante el período 2017-2018.

Fuente: Elaboración propia.

Se realizó la detección microscópica de Cryptosporidium spp. en ejemplares de choritos (M. chilensis), en las cuatro estaciones del año en la Región de Los Lagos.

La mayor prevalencia de Cryptosporidium spp. se registró en la estación invernal con un 67,5 %, en el centro de cultivo de la localidad de Quellón.

En cuanto a la intensidad media de bioacumulación, se obtuvieron los mayores resultados durante las estaciones de otoño e invierno, específicamente en el centro de cultivo de Calbuco con 2,6 ooquistes de Cryptosporidium spp. por ejemplar.

Para los rangos de intensidad ooquística, durante todo el estudio este fluctuó entre 1 a 14 ooquistes de Cryptosporidium spp. observado al microscopio, registrándose la mayor intensidad en un ejemplar de la localidad de Castro durante el muestreo invernal.

En cuanto a la abundancia media de bioacumulación, se obtuvo el mayor resultado en la estación invernal, en las localidades de Calbuco y Quellón, ambas con 1,7 ooquistes de Cryptosporidium spp. por ejemplar.

En cuanto a las estructuras anatómicas del chorito en donde se realizó la detección de ooquistes de Cryptosporidium spp., estas fueron: epitelio del intestino, lumen del intestino, branquia y tejido conjuntivo. Cabe mencionar que todas estas estructuras del marisco son comestibles.

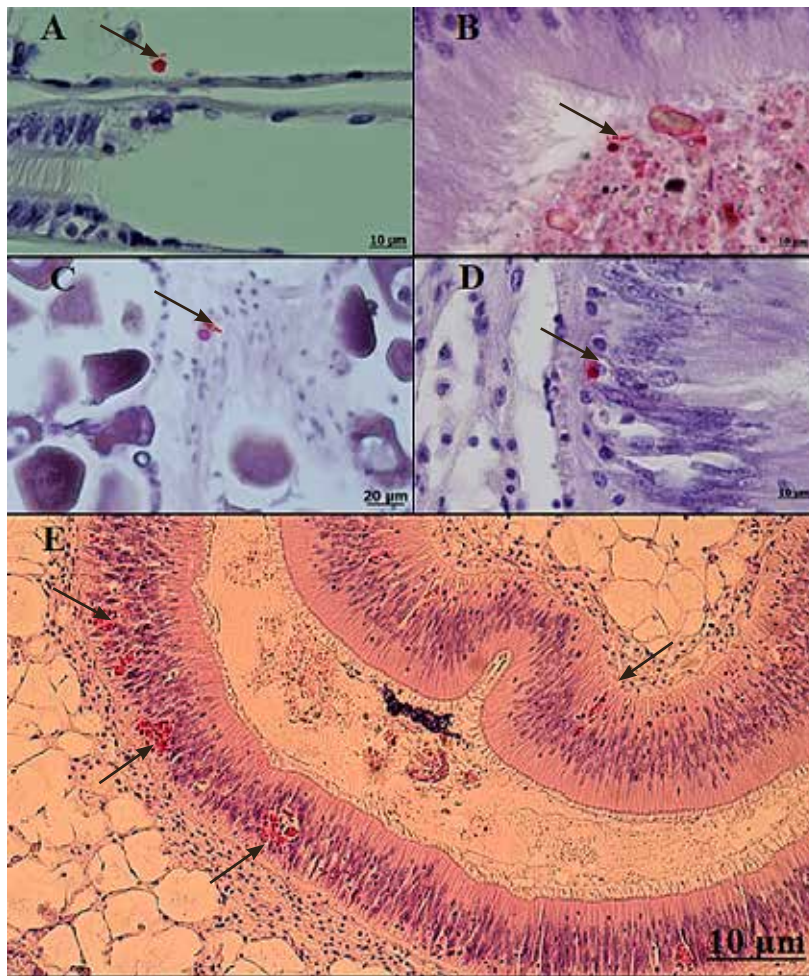


Figura N° 3: Secciones histológicas con la detección microscópica de ooquistes de Cryptosporidium spp. (flechas) en diferentes estructuras anatómicas del marisco (M. chilensis).

Fuente: Fotografías del autor.

A) Branquia (aumento: 100X).
B) Lumen del intestino (aumento: 100X).
C) Tejido conjuntivo (aumento: 40X).
D) Epitelio del intestino (aumento: 100X).
E) Encapsulamiento de ooquistes de Cryptosporidium spp. en epitelio del intestino (aumento: 20X).
Tinción A), B), C), D) y E): Ziehl Neelsen modificado.

CONCLUSIONES FINALES

Los resultados obtenidos en el presente estudio demuestran que el marisco de mayor consumo per cápita en el país, el chorito o mejillón chileno de cultivo (Mytilus chilensis), bioacumula en su interior ooquistes de Cryptosporidium spp.

La detección microscópica del agente parasitario en los ejemplares muestreados, desde centros de cultivo de la Región de Los lagos, Chile, permite concluir que su consumo en crudo podría ocasionar la aparición de casos y/o brotes de criptosporidiosis de origen alimentario, al tratarse del estadio infectivo del parásito (ooquiste).

Se sugiere realizar la transferencia del conocimiento científico de esta detección microscópica de ooquistes de Cryptosporidium spp., efectuada por primera vez en el país, al Ministerio de Salud (MINSAL), para que tomen conocimiento de la presencia del citado agente parasitario, recomendando su análisis y discusión en torno a la factibilidad de una futura incorporación a los parámetros microbiológicos de este grupo de alimento (marisco), en el Reglamento Sanitario de los Alimentos (RSA),[43] ya que actualmente no se encuentra considerado.

Se sugiere, asimismo, realizar la transferencia del conocimiento científico de esta detección a la Autoridad Sanitaria del Ejército (ASE), para su posterior comunicación a nivel institucional, con la finalidad de aumentar los resguardos, tanto al momento de utilizar esta especie como materia prima, como para su correcto consumo al interior de las unidades del Ejército.

BIBLIOGRAFÍA

ARANA. P. (2012). *Recursos pesqueros del mar de Chile*. Valparaíso, Chile. Editorial Universitaria de Valparaíso.

ARREDONDO, C.E. (2014). *Detección de Cryptosporidium spp. en el Pingüino de Magallanes (Spheniscus magellanicus) en dos pingüineras de la Región de Magallanes y Antártica Chilena*. Tesis Pregrado. Universidad de Chile. Santiago, Chile.

BARRIOS, N.S. (2005). *Estudio coproparasitario en primates no humanos del Parque Zoológico de Quilpué, V Región, Chile*. Tesis pregrado. Universidad Austral de Chile. Valdivia, Chile.

BUSH, A.; LAFFERTY, K.; LOTZ, J. & SHOSTAK, A. (1997). Parasitology meets ecology on its own terms: Margolis *et al.* revisited. J. Parasitol.

43 MINISTERIO DE SALUD, Reglamento Sanitario de los Alimentos. DS N° 977/97, Publicado en el Diario Oficial de 13.MAY.97, Santiago, Chile.

DEL COCO, V.F.; CORDOBA, M.A. & BASUALDO, A. (2009). "Criptosporidiosis: una zoonosis emergente". *Revista Argentina de Microbiología*.

DÍAZ-LEE, A.; MOLINA, R.; DOUGNAC, C.; MEERCADO, R.; RETAMAL, P. & FREDES, F. (2015). "Analytical sensitivity of staining and molecular techniques for the detection of Cryptosporidium spp. oocysts isolated from bovines in water samples: a preliminary study". *Archivos de Medicina Veterinaria*.

Ejército de Chile, (1960). Foro de Alimentación: Los problemas alimentarios del Ejército, Dirección de Sanidad Militar, Santiago, Chile.

Ejército de Chile, (1987). Manual de Higiene Ambiental y Control de Alimentos, Comando de Apoyo Logístico, Santiago, Chile.

Ejército de Chile, (2016). Plan de Salud Ambiental 2016-2010, Comando General de Personal, Dirección de Sanidad, Santiago, Chile.

Ejército de Chile, (2008). Manual de Cocina Militar, División Logística, Santiago, Chile.

FAYER, R. & XIAO, L. (2008). *Cryptosporidium and cryptosporidiosis*. Boca Raton, Florida, E.E.U.U. 2nd Edition CRC Press.

FAYER, R. (1994). "Effect of high temperature on infectivity of Cryptosporidium parvum oocysts in water". *Applied and Environmental Microbiology*.

FAYER, R.; TROUT, J.M. & JENKINS, M.C. (1998). "Infectivity of Cryptosporidium parvum oocysts stored in water at environmental temperatures". *Journal of Parasitology*.

FREIRE-SANTOS, F.; OTEIZA-LOPEZ, A.M.; VERGARA-CASTIBLANCO, C.A.; ARES-MAZAS, E.; ALVAREZ-SUAREZ, E. & GARCIA-MARTIN, O. (2000). "Detection of Cryptosporidium oocysts in bivalve mollusks destined for human consumption". *Journal of Parasitology*.

GIANGASPERO, A.; MOLINI, U.; IORIO, R.; TRAVERSA, D.; PAOLETTI, B. & GIASANTE, C. (2005). "Cryptosporidium parvum oocysts in seawater clams (Chamelea gallina) in Italy". *Preventive Veterinary Medicine*.

GOMEZ-BAUTISTA, M.; ORTEGA-MORA, L.M.; TABARES, E.; LOPEZ-RODAS, V. & COSTAS, E. (2000). "Detection of infectious Cryptosporidium parvum oocysts in mussels (Mytilus galloprovincialis) and cockles (Cerastoderma edule)". *Applied and Environmental Microbiology*.

GOMEZ-CUOSO, H. (2006). *Cryptosporidium en moluscos bivalvos*. Tesis PhD, Universidad de Santiago de Compostela. Santiago de Compostela, España.

GOMEZ-CUOSO, H.; MENDES-HERMIDA, F.; CASTRO-HERMIDA, J.A. & ARES-MAZAS, E. (2006). "Cryptosporidium contamination in harvest areas of bivalve molluscs". *Journal of Food Protection*.

GORMAN, T. & GODOY, A. (1989). "Hallazgo de Cryptosporidium spp. en un equino F. S. inglés diarreico". *Monografías de Medicina Veterinaria*.

GORMAN, T.; SOLO, A. & ALCAINO, H. (2006). "Parasitismo gastrointestinal en perros de comunas de Santiago de diferente nivel socioeconómico". *Revista de Parasitología Latinoamericana*.

Ministerio de Salud, (2005). Reglamento sobre Notificación de Enfermedades Transmisibles de Declaración Obligatoria (ENO), DS N° 158/04, Publicado en el Diario Oficial de 10.MAY.05, Santiago, Chile.

Ministerio de Salud, Reglamento Sanitario de los Alimentos. DS N° 977/97, Publicado en el Diario Oficial de 13.MAY.97, Santiago, Chile.

MOLINA, R.; MERCADO, R. & FREDES, F. (2010). "Importancia de la detección del protozoario zoonótico Cryptosporidium parvum en muestras de agua". *Avances en Ciencias Veterinarias*.

NEIRA, P.; MUÑOZ, N.; STANLEY, B.; GOSH, B. & ROSALES, M. (2010). "Cryptosporidium parvum en gastrópodos silvestres como bioindicadores de contaminación fecal en ecosistemas terrestres". *Revista Chilena de Infectología*.

Organización Mundial de la Salud (2001). El control de las enfermedades transmisibles. Washington, EE.UU., Edición N° 17.

PRADO, V.; BRINCK, P. & MARTINEZ, J. (1985). "Enteritis por Cryptosporidium en un paciente leucémico". *Revista Chilena de Pediatría*.

TEXIA, G.; ALCAINO, H. & MANDRY, P. (1990). "Criptosporidiosis en ovinos y caprinos de la zona central de Chile". *Archivos de Medicina Veterinaria*.

LOS PROCESOS ADMINISTRATIVOS DISCIPLINARIOS A NIVEL INSTITUCIONAL Y LA PROFESIONALIZACIÓN DE LA LABOR DEL FISCAL ADMINISTRATIVO: VENTAJAS Y DESAFÍOS[1]

CAPITÁN ANDRÉS GUTIÉRREZ ROMERO[2]

Resumen: *en este trabajo se realiza un análisis de los procesos a través de los cuales se desarrolla la materialización de la potestad disciplinaria de los mandos, a través tanto del expediente disciplinario, como de las investigaciones sumarias administrativas. Para ello se parte con una distinción entre los procedimientos y procesos administrativos, estableciendo la vinculación entre ambos y sus efectos. A continuación, se estudian algunas iniciativas institucionales dispuestas en orden a mejorar la eficiencia para impartir una adecuada justicia en materia disciplinaria viendo sus ventajas y los desafíos que este plantea en el quehacer institucional.*
Palabras clave: *procedimiento administrativo, proceso administrativo, potestad disciplinaria, justicia administrativa.*

Abstract: *this article perfoms an analysis of the processes through which the materialization of the disciplinary authority of the Commands is developed, through both the disciplinary file and through the Summary Administrative Investigations. To this end it will start with a distinction between the procedures and administrative processes, establishing the link between both of them and their effects. Next, some institutional initiatives are studied, arranged in order to improve the efficiency to impart an adequate justice in disciplinary matters, seeing their advantages and the challenges that this poses in the institutional task.*
Keywords: *administrative procedure, administrative process, disciplinary power, administrative justice.*

INTRODUCCIÓN

El ejercicio de las potestades disciplinarias es una cualidad inherente en toda la actividad administrativa del Estado, dado que por regla general estos sistemas siguen el clásico modelo

1 Artículo ganador del tercer puesto del concurso "Desarrollando Capacidades Militares", en el ámbito de recursos humanos y estudios sociales.
2 Oficial del Servicio de Justicia Militar, abogado, magíster en Ciencias Políticas de la Academia Nacional de Estudios Políticos y estratégicos.

establecido por Napoleón,[3] el cual obedece a la estructura jerárquica, característica que es por naturaleza inherente a la profesión militar.

El ejercicio de estas potestades al nivel de las Fuerzas Armadas se encuentra contenido en el DNL-911 "Reglamento de Disciplina para las Fuerzas Armadas", norma que es una cristalización del catálogo de deberes éticos, morales y disciplinarios que deben obedecer los integrantes de los cuerpos castrenses en el ejercicio de sus funciones.[4] Su trasgresión por ende lleva aparejado la configuración de un proceso que no tiene características arbitrales o meramente discrecionales, sino que fuertemente regulado, encausado por el principio de legalidad en ejercicio de la función pública, pero teniéndose en mira la cautela de las garantías más esenciales para su destinatario siendo la más relevante el derecho a un "debido proceso".

Esta garantía se encuentra consagrada en el artículo 19 Nº 3 de nuestra Carta Fundamental, la cual establece *"La igual protección de la ley en el ejercicio de sus derechos"*, siendo la misma norma que señala a continuación que: *"Toda persona tiene derecho a defensa jurídica en la forma que la ley señale y ninguna autoridad o individuo podrá impedir, restringir o perturbar la debida intervención del letrado, si hubiere sido requerida. Tratándose de los integrantes de las Fuerzas Armadas y de Orden y Seguridad Pública, este derecho se regirá, en lo concerniente a lo administrativo y disciplinario, por las normas pertinentes de sus respectivos estatutos"*.

Este último punto reviste un interesante análisis, dado que establece características especiales al régimen disciplinario de las Fuerzas Armadas, es decir, lo extrae del régimen general que se emplea para el resto de la Administración Central del Estado. Estas cualidades y características hacen del sistema disciplinario de las Fuerzas Armadas algo único, pero atendido a las misiones constitucionales que se le otorgan por la Carta Fundamental, las que, en síntesis, requieren que la disciplina sea un valor de capital importancia a la hora de su mantención.

Por otra parte, las investigaciones sumarias administrativas que se desarrollan al interior de las Fuerzas Armadas son procedimientos tendientes a la ejecución de una serie de procesos, diligencias y actuaciones relacionados con la comprobación, por la vía administrativa, de hechos determinados por la autoridad militar que son trascendentes en cuanto a afectar al servicio y que con los medios disponibles asistan dudas sobre las circunstancias en que estos ocurrieron o que los hechos resulten poco evidentes, teniendo como objeto la ejecución de este procedimiento establecer responsabilidades o acreditar causales originarias de algún derecho, atendido el régimen especial disciplinario de las Fuerzas Armadas. Encontramos este procedimiento tratado en el DNL-910 "Reglamento de Investigaciones Sumarias Administrativas de las Fuerzas Armadas", el

3 ALDUNATE, Ramos F. Manual Práctico de Derecho Administrativo. Thomson Reuters, Puntolex. Santiago, Chile, Año 2009.

4 CELIS, Danzinger G. y BARRA, Gallardo N. Manual de Responsabilidad Administrativa. Thompson Reuters Puntolex. Santiago, Chile. Año 2009.

que difiere en su fisionomía y reglas de tramitación al procedimiento general regulado por la Ley Nº 18.834 "Estatuto Administrativo".

El Régimen Disciplinario Militar y la materialización de las infracciones administrativas

Como una perspectiva inicial, y que debe tenerse en cuenta en el escenario nacional actual, la vigencia de la Constitución Política de la República de 1980 y su posterior reforma significó uno de los progresos más importantes, en el que se logró la instauración de un nuevo modelo en el proceso de persecución penal, la denominada "Reforma Procesal Penal", que fue inspirada y articulada bajo la idea central de asegurar la plena vigencia y respeto de los derechos básicos de las personas y que actualmente no concibe ni da cabida a un sistema de imposición de medidas coercitivas sobre las personas sin que se tomen en cuenta previamente las exigencias de racionalidad y justicia que demanda la Constitución. Todos estos principios tienen una aplicación general transversal en toda la actividad del Estado y, por ende, impactan el régimen disciplinario de las Fuerzas Armadas.

No obstante, estas garantías se tienen que conjugar con el bien jurídico a cautelar dentro de las Fuerzas Armadas: la "disciplina", siendo esta esencial dentro de los cuerpos armados, dada la sensible función que les asigna la misma Constitución respecto de la defensa del país. Por este motivo, todo el personal[5] que integra los cuerpos castrenses se encuentra sometido a la acción disciplinaria.

La Ley Orgánica Constitucional de las Fuerzas Armadas, luego de referirse a las misiones que el legislador le encomienda permanentemente para el desarrollo de la Defensa, se enfatiza que: *"El personal que infrinja sus deberes y obligaciones incurrirá en responsabilidad administrativa conforme lo determinen los reglamentos de disciplina y las ordenanzas generales de las respectivas instituciones, sin perjuicio de la responsabilidad civil o penal que pudiere afectarle"*.

Esta norma se encuentra directamente enlazada con el artículo 19 Nº 3 parte final de la Constitución en relación al debido proceso, y la regulación se encuentra armonizada y desarrollada secuencialmente, reforzando, además, la misma Ley Orgánica Constitucional, la idea central de la protección de la disciplina: *"El Ejército, la Armada y la Fuerza Aérea, como cuerpos armados, son esencialmente obedientes, no deliberantes y disciplinados"*.

En atención a estas características especiales, surge la justificación de la existencia de un procedimiento de imposición de medidas disciplinarias con atributos particulares, el que se en-

5 Artículo 3º del DFL 1/1997 (G) Estatuto de Personal de las Fuerzas Armadas.

cuentra contenido en el DNL-910 "Reglamento de Investigaciones Sumarias Administrativas de las Fuerzas Armadas".

En general, el concepto del proceso disciplinario, a nivel de las Fuerzas Armadas, se entiende como: *"aquel conjunto de trámites tendientes a investigar y eventualmente a castigar las presuntas infracciones a normas disciplinarias contenidas principalmente en el DNL-911 "Reglamento de Disciplina para las Fuerzas Armadas", sus cuerpos disciplinarios particulares y en general a las normas que regulan la función pública respecto de los integrantes de las Fuerzas Armadas y/o relaciones a particulares sujetos a un régimen de sujeción que lo contemple".*

Siguiendo las tendencias actuales del tema, en derecho comparado, este concepto se estructura en términos bastante amplios, que abordan todas las opciones y posibilidades de investigación y las sanciones administrativas, incluyéndose en esto las relaciones especiales de sujeción,[6] como las personas privadas de libertad o quienes realizan el Servicio Militar, obligatorio o voluntario, así como aquellos que se encuentren cursando la práctica en alguna institución pública (que dé lugar a un informe negativo de la práctica realizada), como también para ejercer el control respecto del funcionario a cargo de esta.

INTRODUCCIÓN DEL ROL DEL FISCAL ADMINISTRATIVO

Dentro de la configuración de los procesos disciplinarios, la investigación sumaria administrativa regida por el DNL-910 "Reglamento de Investigaciones Sumarias Administrativas de las Fuerzas Armadas" constituye un procedimiento reglado.

A él necesariamente deben ajustarse los funcionarios designados en calidad de fiscal en comisión o responsable de la investigación, lo que, en el desarrollo de su cometido, exige una gran responsabilidad en el cumplimiento de sus funciones, destinado a determinar la ocurrencia de hechos que, eventualmente, representen contravenciones al orden disciplinario y administrativo y, a partir de dicha determinación, a través de la dictación formal de un dictamen fiscal, pueda la autoridad proceder a la ponderación de los hechos que obren en el expediente sumarial para así habilitarlos para la aplicación de medidas disciplinarias, las que pueden significar, en sus casos más extremos, la imposición de medidas expulsivas.

En este contexto, se ha evidenciado un fenómeno de creciente aparición en la vida institucional y que dice relación con la intervención de la defensa letrada de los afectados en el

6 LÓPEZ BENÍTEZ, Mariano, *Naturaleza y presupuestos constitucionales de las relaciones especiales de sujeción,* Civitas/Universidad de Córdoba, Madrid, España, 1994, p. 161 *"…aquellas relaciones jurídico-administrativas caracterizadas por una duradera y efectiva inserción del administrado en la esfera organizativa de la administración, a resultas de la cual queda sometido a un régimen jurídico peculiar que se traduce en especial tratamiento de la libertad y de los derechos fundamentales así como de sus instituciones de garantía, de forma adecuada a los fines típicos de cada relación".*

procedimiento disciplinario, lo que a la luz del Reglamento de Investigaciones Sumarias Administrativas provoca una distorsión respecto de la correcta administración de justicia administrativa.

Esto ocurre porque el fiscal en comisión, como su nombre lo indica, es un funcionario de planta comisionado por la autoridad militar para el cumplimiento de un cometido determinado, el cual está contenido en la resolución de instrucción de la investigación sumaria administrativa.

La aparición de las defensas letradas, es decir, de abogados defensores de los inculpados, plantea una dificultad para la instrucción del procedimiento administrativo, atendido a que la intervención de los oficiales de justicia en la tramitación de dicho procedimiento se encuentra circunscrita a un ámbito netamente de análisis formal de la investigación, norma que se encuentra contenida en el artículo 83 del Reglamento de Investigaciones Sumarias Administrativas.[7] Asimismo, entorpecen, la labor del fiscal en comisión respecto de la articulación de un proceso investigativo exento de fallas,[8] ya que, posteriormente, es cuestionado por parte de estas defensas, las que en una gran medida resultan exitosas,[9] frustrando así el procedimiento administrativo y el objetivo de la investigación, lo que en definitiva provoca un efecto negativo en la esfera disciplinaria institucional, creando una sensación de impunidad.

Por tanto, los estándares actuales de la administración, los conceptos del mando y el devenir de la vida institucional han demandado una reformulación de las investigaciones sumarias administrativas, tomándose como guía esencial la estructuración de un procedimiento directo y expedito, que contribuya a la oportunidad de la determinación de los hechos, de las eventuales responsabilidades que de ello se deriven y, en definitiva, a la aplicación de las medidas que proporcionalmente correspondan.

Para abordar esta problemática a nivel institucional, desde el más alto nivel, se ha dictado la orden de comando que "Crea las Fiscalías Administrativas Permanentes y optimiza procesos y procedimientos para la tramitación de las Investigaciones Sumarias Administrativas",[10] que como fundamentos ha tomado en consideración el importante número de investigaciones sumarias

---

7 Art. 83 DNL-910 "Reglamento de Investigaciones Sumarias Administrativas de las Fuerzas Armadas". Una vez practicadas las diligencias necesarias para establecer los hechos ordenados investigar y, en su caso, para determinar las responsabilidades que pudieren afectar a una o más personas, el fiscal declarará cerrada la investigación, dictando una resolución en tal sentido. Hecho lo anterior, remitirá el expediente a la auditoría que corresponda a dicha repartición o unidad, para su revisión exclusivamente formal y procedimental. Devueltos los antecedentes por la auditoría, y si se formularen observaciones de forma o de procedimiento, el fiscal procederá a subsanar los errores señalados y a realizar las diligencias que correspondan, procediendo luego a redactar personalmente su dictamen.

8 Hay que tener en consideración que los fiscales en comisión son funcionarios de planta y no letrados, que deben distraer gran parte de su tiempo destinado a sus actividades normales de servicio para poder llevar adelante el proceso de investigación, provocando con ello una distracción de esfuerzos dentro de sus labores habituales.

9 Actualmente existe un mercado prolífico respecto de las defensas en materia administrativas de las Fuerzas Armadas, un ejemplo es "Asesoría Administrativas Fuerzas Armadas", donde se encuentran publicadas tarifas y servicios - https://www.facebook.com/asesoriafuerzasarmadas/.

10 Orden Comando CJE SGE DAI a (R) Nº 1000/6717, de fecha 9 de abril de 2015.

administrativas que deben instruirse en las diversas unidades y reparticiones de la institución, el que hace necesario el nombramiento de fiscales y secretarios que deben cumplir estas funciones sin perjuicio de sus misiones específicas, recargando en forma importante las actividades que les corresponde cumplir de acuerdo a su ocupación militar especializada (OME) y jerarquía, lo que ha derivado en una dilación en los plazos de tramitación de las investigaciones sumarias administrativas.

Asimismo, se consideró como fundamento la conveniencia de optimizar y racionalizar los procedimientos relacionados con las investigaciones sumarias administrativas, centralizándolos en un organismo que los instruya, a excepción de aquellos que, por sus características, causas o requerimientos de un organismo extrainstitucional, requieran el nombramiento de un fiscal o secretario especial.

En tal sentido, la unidad pionera de esta estructura ha sido la Brigada de Operaciones Especiales "Lautaro", la cual ha sostenido en el tiempo un número considerable de investigaciones sumarias administrativas,[11] retroalimentando a la Fuerza Terrestre respecto de las experiencias obtenidas, entre ellas, la determinación por parte de los escalones correspondientes de que el cargo de fiscal administrativo fuese servido por parte de un profesional letrado.

Ventajas que presenta la existencia de un fiscal administrativo y de una Fiscalía Administrativa

El funcionario que tiene a su cargo la Fiscalía Administrativa Permanente debe actuar sobre la base de un procedimiento reglado (contenido en el "Reglamento de Investigaciones Sumarias Administrativas" y normas complementarias), en el cual acciona con pleno respeto a los principios de legalidad, discreción, rapidez, imparcialidad y precisión en la redacción de sus providencias y resoluciones, reforzándose con ello las siguientes características que representan un beneficio a nivel institucional:

- Respeto al principio de legalidad: la observancia de este principio obliga al fiscal administrativo no solo a actuar conforme a las normas especiales relacionadas con el procedimiento sumarial contenidas en el respectivo Reglamento de Investigaciones Sumarias Administrativas, sino que, antes de ello, a respetar todo el ordenamiento jurídico administrativo relacionado con este tipo de actuaciones. Este principio se encuentra consagrado en el artículo 7º de la Carta Fundamental.[12]

11 La Brigada de Operaciones Especiales "Lautaro", por su alto grado de entrenamiento y empleabilidad en la Fuerza Terrestre, tiene una generación constante de procesos de investigaciones sumarias administrativas, principalmente por lesiones de entrenamiento, deterioro de material y situaciones disciplinarias.

12 Constitución Política de la República de Chile, artículo 7º. Los órganos del Estado actúan válidamente previa investidura regular de sus integrantes, dentro de su competencia y en la forma que prescriba la ley.

- Discreción en las actuaciones del procedimiento: la intervención del fiscal y sus órganos de investigación debe efectuarse con prudencia y confidencialidad respecto de él o los inculpados, en su actuar general y en relación con la información de la que se tome conocimiento, de manera que los afectados o implicados en el procedimiento sientan que se les otorga garantía de privacidad y que el proceso tendrá carácter de reservado.
- Rapidez de las actuaciones: la naturaleza de la investigación sumaria administrativa, concebida en los términos que establece la reglamentación institucional, obliga a que el fiscal cumpla con su cometido con la mayor diligencia, considerando que la lentitud en el accionar disminuye la apreciación del grado de culpabilidad del afectado, menoscabando y frustrando los fines correctivos y reparadores que se persiguen por esta vía.
- Respeto al principio de imparcialidad de las actuaciones: la actuación del fiscal administrativo, al no tener una relación directa tanto de mando como de subordinación con el afectado, asegura y garantiza conductas y juicios objetivos.
- Precisión en la formulación de las imputaciones: atendido el fenómeno de la aparición de defensas letradas, la labor intelectiva en la articulación de la imputaciones debe realizarse con la máxima cantidad de herramientas metodológicas y técnicas a fin de que se efectúen los reproches disciplinarios en contra de los afectados con el mayor grado de certeza jurídica, teniendo en consideración que la investigación sumaria administrativa se trata de una materia delicada y compleja, y que de presentar falencias, es rápidamente explotada y aprovechada por las defensas de los afectados. En consecuencia, resulta relevante juzgar el mérito y conveniencia de profesionalizar la labor del fiscal administrativo, sobre todo porque los cargos que se contienen en el dictamen fiscal constituyen la representación formal de la conducta del afectado para la configuración de la infracción disciplinaria y/o administrativa, la que debe basarse en una descripción objetiva y precisa de la conducta, y en los antecedentes que consten en el sumario.

Desafíos que se presentan en la labor del fiscal administrativo y en las fiscalías administrativas

Uno de los desafíos más importantes que se plantea respecto a la labor del fiscal administrativo es la mejora continua, dado que dicha autoridad debe distinguirse por su habilidad y pericia para hacer posible el trabajo investigativo, conjugando su conocimiento profesional, base y práctico. Mediante la formación superior, especializaciones, postgrados, cursos y diplomados, la participación en eventos académicos, el fiscal administrativo adquiere las bases conceptuales que le permiten construir, en forma articulada, su conocimiento profesional, relacionándolo con su conocimiento base y práctico por medio de dicha preparación continua y reflexiva.

Figura N° 1. Proceso de formación continua.

Fuente: Elaboración propia.

Lo anterior se constituye como herramientas invaluables dentro del ejercicio de la función investigativa, redundando en una investigación sólida, acabada y con estricto apego a la legalidad vigente.

Otro desafío que se presenta dentro del panorama de la labor del fiscal administrativo, y su profesionalización, es incrementar la independencia y transparencia en la instrucción de las investigaciones sumarias administrativas,[13] como asimismo su integración a la estructura orgánica institucional. Actualmente estas solamente ejercen sus atribuciones en una esfera muy reducida,[14] siendo un desafío a futuro su implementación homogénea a través de los diversos estamentos institucionales, siendo un factor a ponderar que estas sean integradas por profesionales letrados, que representen un contrapeso respecto del fenómeno de defensas letradas, cada vez más presente en el quehacer institucional.

Lo anterior en el entendido de que se debe tender a la profesionalización de esta sensible función institucional, con el nombramiento de fiscales administrativos de acuerdo a criterios de especialización y no solo por el hecho de ser personal de planta, sumado al proceso de innovación[15] que impera a nivel de la administración del Estado.

CONCLUSIONES

En este breve panorama, al evidenciarse y ser incontrovertible el hecho de que cada vez más los afectados por un proceso disciplinario a nivel institucional recurren a defensas letradas, así como también la necesidad de racionalizar los procesos en que se tramitan las investigaciones

13 Sobre este tema resulta útil señalar la Orden General Nº 002385 de fecha 6 de enero de 2016 de la Dirección General de Carabineros de Chile, FISCALÍAS ADMINISTRATIVAS: Crea las que indica y determina competencia a nivel nacional. - http://www.carabineros.cl/transparencia/og/ OG2385_08022016.pdf

14 A la fecha se encuentran activas las fiscalías administrativas permanentes de Arica, Iquique y de la Brigada de Operaciones Especiales "Lautaro".

15 Este punto resulta interesante a nivel de administración central respecto de la aplicación de las tecnologías de la información y de los sistemas de tramitación electrónica, a nivel institucional se está implementando el sistema de ingreso de ISAs a través de la plataforma Sistema Institucional de Administración de Personal (SIAP).

sumarias administrativas y el dar un estricto cumplimiento a los principios de legalidad, objetividad y transparencia, se ha derivado en la conformación de las Fiscalías Administrativas Permanentes, dándole una preponderancia al rol y profesionalización del fiscal administrativo.

Ello representa la implementación tangible de las medidas del escalón superior para lograr una mejor sustanciación y calidad de las investigaciones sumarias administrativas, frente a un entorno administrativo que se torna dinámico y cambiante, con un gran acento en los derechos de las personas y el control ciudadano de la actividad de la administración.

Lo anterior redunda en un reforzamiento de las políticas de la institución; en conceptos emitidos por los más altos niveles institucionales en orden a mejorar la efectividad de las investigaciones; en la adecuada imposición de medidas disciplinarias que de cada caso se desprendan; en una objetividad respecto de la formulación de los cargos y de las circunstancias que atenúan la responsabilidad o la eximan; y, finalmente, en que ante las defensas letradas haya legítimamente la presencia de una contraparte (fiscal y defensa) y una autoridad administrativa llamada a resolver como un tercero ajeno en su función de dictar justicia en materia administrativa y/o disciplinaria.

BIBLIOGRAFÍA

ALDUNATE RAMOS, F. (2009). *Manual Práctico de Derecho Administrativo*. Thomson Reuters, Puntolex. Santiago, Chile.

CELIS DANZINGER, G. y BARRA GALLARDO, N. (2009*). Manual de Responsabilidad Administrativa*. Thompson Reuters Puntolex. Santiago, Chile.

LÓPEZ, Mariano (1994). *Naturaleza y presupuestos constitucionales de las relaciones especiales de sujeción*. Civitas/Universidad de Córdoba, Madrid, España.

PLANCHADELL GARGALLO, A. (1999). *El Derecho Fundamental a ser informado de la acusación*. Editorial Tirant Lo Blanch. Valencia, España.

SAN MARTÍN CERRUTI, M. (2010). *Sumario Administrativo regulado por el Estatuto Administrativo contemplado en la Ley 18.834*. III Versión Seminarios Probidad y Transparencia para la Administración.

SANTAMARÍA PASTOR, J. (2002). *Principios de Derecho Administrativo*. Volumen II. 3º Edición. Colección Ceura. Editorial Centro de Estudios Ramón Areces S.A. Madrid, España.

ROMÁN CORDERO, C. (2008). *Derecho Administrativo Sancionador: ¿Ser o no ser? He ahí el dilema*. En: Pantoja Bauzá, Rolando (coord.) (2008). Derecho Administrativo: 120 años de cátedra. 1ª edición, Santiago, Editorial Jurídica de Chile.

Legislación

Constitución Política de la República.

Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

Ley Nº 18.948, Orgánica Constitucional de las Fuerzas Armadas.

DFL Nº 1/1997 (G) "Estatuto de Personal de las Fuerzas Armadas".

Ley Nº 19.880 que establece "Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado".

DNL-910 "Reglamento de Investigaciones Sumarias Administrativas de las Fuerzas Armadas".

Orden Comando CJE SGE DAI a (R) Nº 1000/6717, de fecha 9 de abril de 2015.

Publicaciones en Internet

Dirección General de Carabineros de Chile, FISCALÍAS ADMINISTRATIVAS: Crea las que indica y determina competencia a nivel nacional. Recuperada en: http://www.carabineros.cl /transparencia/og/OG2385_08022016.pdf (27 de septiembre de 2018).

"Asesorías Administrativas Fuerzas Armadas". Recuperada en: https://www.facebook.com/asesoriafuerzasarmadas/. (27 de septiembre de 2018).

LA MEDICIÓN DE LA INTELIGENCIA EMOCIONAL COMO FACTOR COMPLEMENTARIO A LA EVALUACIÓN DEL MÉRITO MILITAR EN LA DESIGNACIÓN DE LOS MANDOS[1]

TENIENTE MAÍTY VERA BUSTOS[2]

Resumen: *en el ámbito de la administración de personal, en particular en la asignación de mandos, cabe preguntarse si, además de los hechos que puntúa el mérito militar, es posible agregar otro factor de análisis que pueda distinguir entre dos sujetos de similar carrera, pero con distinta forma de interactuar con el medio que los rodea. En este orden de ideas, surge la utilización del constructo psicológico de la inteligencia emocional como factor de evaluación referencial para los futuros mandos y su aplicación a través del test MSCEIT.*
Palabras clave: *inteligencia emocional, liderazgo, mando, toma de decisiones.*

Abstract: *in the area of human resources, particulary, in the assignment of commands, it is possible to ask whether, in addition to the facts that merit military scores, it is possible to add another factor of analysis, one that can distinguish between two subjects of similar career, but with a different way of interacting with the environment that surrounds them. In this order of ideas, the use of the psychological construct of emotional intelligence as a factor of referential evaluation for future managers and its application through the MSCEIT test emerges.*
Keywords: *emotonial intelligence, leaders ship, command, dicision making.*

INTRODUCCIÓN

La cartilla de Evaluación al Mérito Militar surge en el ámbito de la administración de personal: *"estableciendo procedimientos, normas y condiciones a considerar en los procesos de selección de oficiales y cuadro permanente para desempeñar cargos, comisiones y/o cursos*

1 Artículo ganador del tercer puesto del concurso "Desarrollando Capacidades Militares", en el ámbito de Recursos Humanos y Estudios Sociales.

2 Oficial del Servicio de Personal, diplomada en Gestión de Recursos Humanos y en Gestión y Administración Pública de la Universidad Bernardo O´Higgins, actualmente alumna de psicología en la Universidad de las Américas.

de perfeccionamiento en el país y en el extranjero, con el objeto que sean designados sobre la base de sus méritos".[3]

Para alcanzar este propósito, se determinaron parámetros que evalúan hechos concretos, permitiendo con esto una imagen nítida del desempeño del personal a lo largo de su carrera militar, buscando además garantizar principios de transparencia, equidad y justicia.

Estas medidas constituyen la base para la selección, existiendo otros factores que también interactúan en el proceso, siendo finalmente una herramienta referencial para la elección, recayendo en la figura del comandante en jefe del Ejército la decisión de quién desempeñará cargos del orden del ejercicio del mando y aquellos de valoración de mérito: *"el CJE tiene la potestad para designar a cualquier oficial y/o cuadro permanente que se encuentre en condición de disponibilidad y que se estime idóneo para desempeñar dichos cargos".*[4]

De lo ya expuesto, es menester preguntarse si a los elementos de la cartilla de Evaluación al Mérito Militar, que como ya se señaló miden hechos (calificaciones, puestos, logros académicos), es posible agregar otra herramienta, complementaria y referencial, que permita distinguir entre un sujeto A y B, similares en mérito, pero diferentes en sus características personales, y de ser así ¿qué técnica científica podría contribuir en este proceso?

Para desarrollar el presente artículo fue motivo de inspiración un estudio realizado a los trabajadores estrella de los connotados laboratorios Bell, de Princeton.

Ahí trabajan ingenieros y científicos cuyo coeficiente intelectual académico es extraordinariamente elevado. Dentro de este pozo de talentos, fue posible evidenciar que algunos de ellos sí eran verdaderas "estrellas" en términos de rendimiento, mientras que otros alcanzaban resultados más bien mediocres. Pues bien, la investigación arrojó que la diferencia entre unos y otros no radica tanto en su CI académico como en su CI emocional y que los trabajadores "estrella" eran personas más capaces de motivarse a sí mismas y más dispuestas a organizar sus redes informales en equipos *ad hoc.*[5]

Dado lo anteriormente señalado, este artículo tendrá por objetivo considerar la inteligencia emocional y su evaluación en los futuros mandos como propuesta de una herramienta complementaria a la cartilla de Evaluación al Mérito Militar y referencial para la decisión final del CJE.

---

3 EJÉRCITO DE CHILE: cartilla de "Evaluación al Mérito Militar", Santiago, Chile, División Doctrina, 2015, p. 9.
4 *Ibídem,* pp. 2-4.
5 GOLEMAN, D. (1996). *Inteligencia Emocional,* Barcelona, España, Ed. Kairos, p.140.

Es por ello que, desde el ámbito del recurso humano, selección de personal, revisaremos en primera instancia el concepto de inteligencia emocional, su relación con el liderazgo, la toma de decisiones y el mando, para finalmente plantear el "Mayer-Salovey-Caruso Emotional Intelligence Test" (MSCEIT) como parámetro científico capaz de cuantificar el CI emocional.

CONCEPTO DE INTELIGENCIA EMOCIONAL

Utilizando el sentido común es posible desestimar la posibilidad de que exista alguien que no desee ser catalogado de inteligente, pero ¿qué es la inteligencia?, es difícil responder a esto en la actualidad. Rosas Boetto y Jordan señalan que hay múltiples definiciones y no es tan fácil determinar cuál es más certera; incluso es posible decir que todas pueden ser igualmente falsas o válidas.[6] En la cultura griega, por ejemplo, se distinguía entre dos tipos de inteligencia: "nous" y "metis", siendo Atenea representativa de las características de la primera, que es esencialmente parmenídea (capacidad para organizar el mundo abstracto, estático e impersonal de relaciones invariantes). La otra forma de inteligencia, metís, esencialmente heráclitea, estaba más ligada a los contextos interpersonales, la cual requería de la comprensión de claves sutiles en la relación con otras personas.[7] Esta última fue invisibilizada por la psicología científica por muchos años, siendo Goleman y Damasio sus más grandes exponentes.

Entonces, ¿qué es la inteligencia emocional (IE)? En las palabras del ilustre psicólogo chileno y doctor en Psicología Cognitiva, Ricardo Rosas, sería la metahabilidad que determina el éxito con que podemos utilizar otras capacidades, entre las que se incluyen el intelecto puro.[8]

Por su parte, Goleman señala que son otras características personales que escapan al intelecto puro, como la capacidad de motivarnos a nosotros mismos, de perseverar en el empeño a pesar de las posibles frustraciones, de controlar los impulsos, de diferir las gratificaciones, de regular nuestros propios estados de ánimo, de evitar que la angustia interfiera con nuestras facultades racionales y, por último, la capacidad de enfatizar y confiar en los demás.[9]

Por otra parte, el afamado neurólogo portugués Antonio Damasio no habla del concepto inteligencia emocional como tal, pero nos da luces sobre la importancia de la regulación de emociones y sentimientos en los procesos de toma de decisiones. Finalmente, Salovey y Mayer conciben la IE como una inteligencia genuina basada en el uso adaptativo de las emociones y su aplicación a nuestro pensamiento.

---

6 ROSAS, Ricardo; BOETTO, Carolina; JORDÁN, Verónica (2005). *Introducción a la psicología de la inteligencia,* Santiago, Chile, Ediciones Universidad Católica de Chile, p. 16.

7 *Ibídem*, p. 15.

8 *Ibídem*, p. 96.

9 GOLEMAN, Daniel (1996). *Inteligencia Emocional,* Barcelona, España, Ediciones Kairós, p. 68.

LA INTELIGENCIA EMOCIONAL, EL LIDERAZGO Y LA TOMA DECISIONES

El pensar en la inteligencia emocional como factor de evaluación referencial para la designación de los mandos resulta del análisis mismo, tanto de su significado, como de los elementos que componen el ejercicio de la autoridad, que implícitamente requiere la toma de decisiones y el liderazgo.[10]

Por tanto, desde una lógica instrumental, si queremos seleccionar personas que encarnen el ideal del mando, debemos evaluar el constructo psicológico de estas dos ideas, es decir, la inteligencia emocional. Dicho de otra forma, si los elementos del mando fuesen números fraccionarios en una ecuación, el común denominador de ambos sería la IE.

La justificación para señalar que la inteligencia emocional es vinculante al liderazgo está dada por el mismo concepto, presente en nuestra doctrina: el arte de influir sobre los demás, lograr de ellos la adhesión a un ideal para que, provistos de un propósito, dirección y motivación, desarrollen una tarea, cumplan una misión y mejora en la organización, sintiéndose al mismo tiempo satisfechos y realizados.[11]

Para la operacionalización de esta idea, el Ejército define los atributos y competencias de un líder, los que, al ser comparados con el modelo de Goleman de IE, muestran una correlación entre los aspectos emocionales, de atributos y competencias, como aparece en las figuras 1 y 2. Por tanto, la inteligencia emocional es la condición *sine qua non* del liderazgo.[12]

Figura N° 1: Dimensión del Hacer, del Modelo Integral de Liderazgo RDE-11.

Fuente: RDE-11. Reglamento de Liderazgo del Ejército.

10 Ejército de Chile: RDM-20001 Reglamento. "Mando Y Control", Santiago, Chile, División Doctrina, 2014, p. 27.

11 Harvard Business Review [En línea] (Fecha de consulta: 24 de septiembre de 2018). Disponible en: https://danielcaballol.files.wordpress.com/2009/10/hbrla.pdf

12 Ejército de Chile: RDL "Modelo integral de liderazgo del Ejército de Chile", Santiago, Chile, División Doctrina, 2014, p. 9.

COMPETENCIA PERSONAL		COMPETENCIA SOCIAL	
Autoconcienciación	**Autoadministración**	**Concienciación social**	**Administración de la relación**
- Autoconciencia emocional Autoconcienciación - Autoevaluación Autopreparación - Seguridad de sí mismo Tranquilo, seguro de sí mismo Carácter distintivo del guerrero Versado Porte militar	- Autocontrol emocional - Transparencia - Adaptabilidad Resistencia Agilidad mental - Logros - Iniciativa Innovación - Optimismo Crea un ambiente positivo Buena forma física	- Concienciación organizativa Valores del Ejército - Servicio - Empatía	- Liderazgo de inspiración Lidera con el ejemplo - Influencia Extiende la influencia Lidera a otros Se comunica - Capacita a otros Capacita a líderes - Catalizador del cambio Crea un ambiente positivo - Administración de conflictos Tacto interpersonal Buen juicio - Trabajo en equipo-cooperación Obtiene resultados

Figura N° 2: Modelo de requisitos de liderazgo y el modelo de comparación de Goleman.

Fuente: Harvard Business Review.

Un segundo elemento de análisis es la inteligencia emocional y la toma de decisiones, en este punto, el neurobiólogo Antonio Damasio nos entrega sus aportes. Para ilustrarnos sobre la relación entre las emociones y la toma de decisiones utiliza el célebre caso de Phineas P. Gage, quien era un capataz de la construcción que, a sus veinticinco años, protagonizó un accidente en el que una varilla de hierro lesionó la parte prefrontal de su cerebro. A pesar de lo estrepitoso del accidente, Gage sobrevive, camina, habla y ríe como si aparentemente no le hubiese pasado nada. A lo menos esa fue la primera impresión luego del accidente, pero en el transcurso de los días, todos los que conocían a Gage llegarían a la misma conclusión: ¡Gage, ya no era Gage! El individuo puntual, brillante y comprometido ahora era todo lo contrario. ¿Qué le había sucedido? La lesión cerebral sufrida provocó que, mientras los procesos cognitivos representantes del intelecto, como son la planificación, la abstracción, el lenguaje y la memoria de trabajo, entre otros, no fueron afectados, manteniéndose incluso el conocimiento de las convenciones sociales, la práctica de esta última se vio altamente alterada a causa de una lesión cerebral en la corteza prefrontal ventromedial (CPVM).

Por tanto, el comportamiento de Gage no se debía a las decisiones de una mente disminuida, sino a las decisiones de una mente miope al futuro, que tenía un conocimiento sobre los

valores sociales en abstracto, pero que estaban desunidos de la vida real. En la situación antes descrita, el sujeto vio comprometida su capacidad de comportarse según las normas sociales que anteriormente había aprendido, producto del daño en la CPVM, una región crítica para la toma normal de decisiones.[13]

El lenguaje técnico que Damasio utiliza para señalar lo acontecido a Gage es: el aparataje de la racionalidad, que tradicionalmente se suponía neocortical, parece no funcionar sin el de la regulación biológica, que por su parte se conjeturaba subcortical. La naturaleza no solo parece haber construido el aparataje racional encima del herramental biológico-regulatorio, sino que con y a partir de él. Por tanto, no puede haber razón sin emoción.

Damasio va un poco más allá, señalando que el organismo debe constantemente evaluar y tomar decisiones, en base a la multiplicidad de escenarios posibles, sobre una enorme cantidad de información. Así pues, si pretendiésemos utilizar la lógica costo-beneficio, fracasaríamos o perderíamos demasiado tiempo, dado que la atención y la memoria operativa no tienen la capacidad suficiente para procesar tanta información.

Por tanto, la guía que nos brindan los sentimientos, y que la pura razón no nos puede proporcionar, se basa en el proceso de "marcar" imágenes o escenarios posibles de acción, dentro de la variedad de imágenes que surgen al razonamiento, relativas a determinados estados "somáticos", dándoles un carácter de positivos o negativos como opción, categorizando el conocimiento fáctico, brindando señales de alerta, evitando una línea de acción que nos conduzca a un resultado negativo o guiándonos hacia uno positivo.

Solo después de que el "marcador somático" ha disminuido drásticamente el número de opciones, se puede realizar un análisis del tipo costo-beneficio o cualquier otro tipo de proceso de razonamiento.[14]

En consecuencia, la emoción tiene una base biológica en la toma de decisiones, estando directamente ligada a la perspectiva de la IE y la imperiosa necesidad de hacernos sujetos conscientes de esta, ambos pilares angulares del mando.

"MAYER-SALOVEY-CARUSO EMOTIONAL INTELLIGENCE TEST" (MSCEIT)

Durante el desarrollo argumentativo de este trabajo, se ha hablado ampliamente de la inteligencia emocional y de su importancia para el mando, pero, en lo concreto, es necesario señalar

13 ROSAS, Ricardo; BOETTO, Carolina; JORDÁN, Verónica (2005). *Introducción a la Psicología de la Inteligencia,* Santiago, Chile, Ediciones Universidad Católica de Chile, p. 102.

14 *Ibídem,* p.105.

una medida científica que nos permita discriminar entre un sujeto A y B, asignándole un puntaje, como sucede en los test de inteligencia. En esa lógica surge el MSCEIT, una prueba diseñada para evaluar la inteligencia emocional entendida como una capacidad. No se trata de un autoinforme, sino de una prueba de habilidad cuyas respuestas representan aptitudes reales para resolver problemas emocionales.

Es la primera medida que proporciona puntuaciones válidas y fiables en cada una de las cuatro áreas principales de la inteligencia emocional según el modelo de Mayer y Salovey: 1) Percepción emocional, 2) Facilitación emocional, 3) Comprensión emocional y 4) Manejo emocional.[15]

Es posible, gracias a esta medida, evitar las dificultades de elementos descriptivos suscritos por los evaluados o la subjetividad en las evaluaciones de 180° o 360°, donde los resultados obtenidos se basan en la creencia u observación de otro sobre la capacidad del sujeto analizado en la ejecución de una tarea.

El MSCEIT v. 2.0 está compuesto por 141 ítems, diseñados para medir los cuatro factores del modelo; a los evaluados se les pide que completen un total de ocho tareas emocionales de distinta índole, que recogen las habilidades del modelo, entregando un puntaje total, dos resultados asociados a las áreas experiencial y estratégica, los factores correspondientes a las cuatro habilidades del modelo y, finalmente, el puntaje en cada una de sus subescalas.

Cada una de estas puntuaciones es obtenida mediante dos criterios: experto y consenso. El criterio experto implica el grado de acuerdo de la respuesta de los participantes con la opinión de 21 expertos e investigadores en el campo emocional. El criterio consenso se refiere al acuerdo de las respuestas de los participantes de una muestra amplia y heterogénea de más de 5.000 individuos.

Cada una de las cuatro habilidades es medida a través de dos tareas: por ejemplo, la capacidad para percibir emociones es evaluada mediante trabajos de percepción de emociones en rostros faciales y fotografías; el factor de asimilación emocional es estimado con tareas de sensación y facilitación; la capacidad de comprensión de emociones es medida usando tareas de combinación de emociones y otra de cambios o transformaciones emocionales; y, por último, la capacidad para manejar emociones es juzgada mediante actividades de manejo emocional y de relaciones emocionales.[16]

---

15 SELCAP [En línea] (Fecha de consulta: 24 de septiembre de 2018). Disponible en: https://www.selcap.cl/producto/msceit-test-de-inteligencia-emocional-mayer-salovey-caruso/

16 FERNÁNDEZ BERROCAL, Pablo; EXTREMERA PACHECO, Natalio. "La Inteligencia Emocional y la educación de las emociones desde el Modelo de Mayer y Salovey". *Revista Interuniversitaria de Formación del Profesorado,* vol. 19, (núm. 3), p. 63, diciembre 2005.

Figura N° 3: Ejemplo de un ítem de percepción emocional MSCEIT.

Fuente: Imagen del test MSCEIP de Mayer Solovy-Caruso.

CONSIDERACIONES FINALES

No existe emoción sin razón, como tampoco es posible concebir el liderazgo sin la presencia intrínseca de algún grado de inteligencia emocional. En esta premisa radica la idea de adoptar el test MSCEIT como método complementario a la evaluación del mérito militar, para entregar una herramienta referencial en la designación de los mandos de la institución, permitiendo esta prueba medir la diferencia entre sujetos de análogos méritos (hechos formales), pero diferentes en su actuar y forma de relacionarse con otros. Como corolario es dable señalar que no basta ser considerados inteligentes en los términos formales de CI cognitivo, es imperante para el mando también tener una conducta inteligente en términos sociales y personales. Lo anterior, no solamente debido al quiebre de paradigmas que provocó Goleman y Damasio, sino también, a que el manejo de la emoción y su adecuación constituyen una conducta primitiva, propia de nuestra filogenia, destinada a superar los desafíos de la existencia humana.

BIBLIOGRAFÍA

FERNÁNDEZ BERROCAL, Pablo; EXTREMERA PACHECO, Natalio (2005). "La inteligencia emocional y la educación de las emociones desde el modelo de Mayer y Salovey". *Revista Interuniversitaria de Formación del Profesorado*.

ROSAS, Ricardo; BOETTO, Carolina; JORDÁN, Verónica (2005). *Introducción a la psicología de la inteligencia*. Santiago, Chile, Ediciones Universidad Católica de Chile.

Ejército de Chile (2014). RDL "Modelo integral de liderazgo del Ejército de Chile", Santiago, Chile, División Doctrina.

GOLEMAN, Daniel (1996). *Inteligencia Emocional*. Barcelona, España, Ediciones Kairós.

Ejército de Chile (2014). RDM-20001, REGLAMENTO "MANDO Y CONTROL", Santiago, Chile, División Doctrina.

HARVARD BUSINESS REVIEW [En línea] (Fecha de consulta: 24 de septiembre de 2018). Disponible en: https://danielcaballol.files.wordpress.com/2009/10/ hbrla.pdf

CIENCIAS MILITARES, COMBATE, GENERACIÓN DE DOCTRINA Y DOCENCIA

MEMORIAL
DEL
Ejército de Chile

DISEÑO Y DESARROLLO DE UNA PLATAFORMA COLABORATIVA PARA EL CONTROL DE UNIDADES CIVILES Y MILITARES EN EMERGENCIA[1]

MAYOR JORGE VÁSQUEZ ALBORNOZ[2]

Resumen: *el desafío de aportar tecnológicamente al entrenamiento de los Cuarteles Generales de Emergencia mediante el análisis de capacidades militares fue el motor para la creación de un producto que reúne algoritmos de optimización sobre una base de visualización geográfica gratuita asequible. Se propone entrenar la toma de decisiones de los comandantes en situaciones de emergencia a través de una plataforma web y móvil colaborativa y con eso contribuir a dos áreas de misión específicas del Ejército.*
Palabras clave: *aplicación web, colaborativa, emergencia, multi-agencial, informática.*

Abstract: *the challenge to contribute technologically to the training of the General Headquarters of Emergency through the analysis of military capabilities, led us to the creation of a product that brings together on a basis of display optimization algorithms within reach athaud. Through a collaborative web and mobile platform we want to train commanders emergency decision-making cycle and with that, contribute to two specific mission areas of the Army.*
Keywords: *collaborative, web application, emergency, multiagency, computer science.*

INTRODUCCIÓN

El carácter incierto, la premura en la acción el riesgo y la demanda de la población civil por apoyo para el rescate y la protección son algunos de los elementos que se conjugan en una catástrofe de origen natural, como los terremotos, o humano, como pueden ser los incendios. Además,

1 Artículo ganador del primer puesto del concurso "Desarrollando Capacidades Militares", en el ámbito de Ciencias Militares, Combate, Generación de Doctrina y Docencia.

2 Ingeniero Politécnico Militar en Sistemas de Armas, mención Mecánica, profesor de academia en Ciencias de los Materiales, magíster en Ciencia de la Ingeniería Mecánica y magíster en Ciencias en Diseño Computacional y Fabricación, de la Universidad Carnegie Mellon de Estados Unidos de América.

a la amplitud y variedad de los escenarios posibles se deben agregar toda clase de disfunciones, que van desde las telecomunicaciones hasta el transporte de medios de un lugar a otro, pasando por la ejecución de tareas complementarias entre entidades que suelen actuar, la mayor parte del tiempo, de manera independiente y con funciones o medios de naturaleza divergente.

La experiencia adquirida en las tareas realizadas durante los eventos de los últimos años ha dado cuenta de que los tiempos entre acciones relevantes pueden resultar inconducentes y en algunos casos, fatales.

En este contexto, el Ejército es uno de los actores fundamentales en el marco de la respuesta estatal a la demanda civil por ayuda. Como tal, y habida cuenta de que su propósito esencial (la defensa de la soberanía nacional) no coincide plenamente con la estructura de respuesta a situaciones como las descritas, debe generar —por contrapartida— una capacidad de respuesta que satisfaga los requerimientos que se vayan presentando. Una manera de abordar el fenómeno es mediante el reconocimiento de algunas características que son propias de la institución y que se concretan en dos instancias: una interna y otra externa.

La instancia interna es la que dice relación con el conjunto de procedimientos institucionales para abordar tareas que impliquen el empleo de la Fuerza Terrestre (FT), las estructuras de que se vale para ello, las relaciones de mando, las experiencias acumuladas y las opiniones de los expertos.

La instancia externa, por su parte, es dada por el entorno en que ocurre la acción del Ejército, a saber, la ciudadanía o la parte de ella que fue afectada por una emergencia o catástrofe, la autoridad a cargo de la acción del Estado (que en el nivel más alto es el ministro del Interior) en apoyo a la comunidad, el organismo encargado de coordinar la acción de todos los entes que participan del sistema de protección civil (la Oficina Nacional de Emergencia, ONEMI), y todos los otros organismos que contribuyen a reducir los efectos, mitigar los riesgos y canalizar la ayuda solidaria del resto de la sociedad hacia los más afectados.

Estas dos instancias dan cuenta de una realidad global: el Ejército posee una capacidad preexistente, una estructura que le permite no solo integrarse, sino que, además, contribuir al esfuerzo y la acción del Estado.

Estas otras capacidades se agrupan en las denominadas Operaciones Militares Distintas a la Guerra (MOOTW, por sus siglas en inglés), y son ellas las que, preparadas convenientemente, le permiten al Ejército comprometerse y actuar.

Esta preparación no solo implica la planificación, sino que también la capacitación y el entrenamiento. Combatir incendios o rescatar personas arrastradas por un río no son tareas que puedan asumir organismos que no cuenten con la preparación adecuada. Por otra parte, hacer coincidir el

tipo de problema con la solución específica para ese tipo implica una serie de coordinaciones que, según las conclusiones arrojadas en el estudio realizado por el Centro de Modelación y Simulación del Ejército (CEMSE), pueden reducirse en el número y acortarse en el tiempo, lo que hace más oportuna y efectiva la respuesta. El presente artículo explora y describe una aplicación que facilitaría significativamente la respuesta institucional y, con ello, la posibilidad de estar a tiempo en el lugar correspondiente y con los medios adecuados.

LECCIONES APRENDIDAS

El Centro de Lecciones Aprendidas (CELAE) ha generado distintas publicaciones de lecciones aprendidas. Este artículo destaca dos de ellas: el terremoto del 27 de febrero de 2010 y los incendios de 2017.

El año 2010 el Ejército puso a prueba el concepto de Operaciones Militares Distintas a la Guerra (MOOTW), definido en su doctrina operacional.[3] El terremoto del día 27 de febrero determinó el empleo de gran cantidad de medios militares, los que debieron absorber el impacto de la emergencia misma, tanto en el día en que esta se produjo como en las semanas y meses posteriores.

Con respecto a los incendios del año 2017, estos afectaron a siete regiones en total, aunque con efectos distintos al terremoto, en tanto no significaron la pérdida de vidas humanas o de inmuebles a la escala en que lo hizo el terremoto de 2010. Por otra parte, si bien los efectos de la deforestación hacen de los incendios en general un fenómeno cualitativamente distinto al de los terremotos o tsunamis, el tipo de daño que producen puede resultar incluso más grave. Un informe elaborado por dos expertos en la materia, publicado en febrero de 2017 en el diario electrónico CIPER, ejemplifica esta relación cualitativa comparando el incendio de una casa con el de un bosque.

Para efectos de este trabajo, la enseñanza más importante dejada por estos incendios es que se dio un elemento diferenciador clave con respecto al pasado, a saber, la estructuración —antes del evento— de una fuerza de tarea específica. En otras palabras, el Ejército ya contaba con parte de su fuerza (no toda, recordemos que la función esencial del Ejército es la defensa de la soberanía nacional) designada y capacitada para combatir emergencias y catástrofes, por lo tanto, no debió organizarla a medida que se presentaban los eventos. Este cambio cualitativo marca una diferencia importante entre el antiguo modo de operar y el presente.

Sin embargo, las experiencias demostraron que el ataque masivo a un fenómeno como el de los incendios implicaba una coordinación igualmente masiva de los medios. Coordinar medios es mucho más difícil y entrampado que sencillamente designarlos y darles misiones. No solo porque

3 Centro de Lecciones Aprendidas. El empleo de la Fuerza Terrestre en la operación 27F, Santiago, Chile, División Doctrina, 2017, p. 9.

supone la orquestación en tiempo y espacio de un conjunto de acciones distintas que dan por resultado una sola intención global, que es el estado final deseado, sino porque el número de relaciones que se dan entre distintos nodos o partes de una estructura es mucho mayor que el de los nodos mismos. Hay una expresión matemática que dice que dado un número n de nodos, si cada nodo se encuentra conectado a todos los otros, entonces el número de conexiones será igual a $(n \times (n-1)) \div 2$.[4] Así, si se tienen dos nodos, el número de relaciones será igual a $(2 \times (2-1)) \div 2 = 1$. Si se tienen 3, el número será igual a 3; si se tienen 4, el número será igual a 6; si se tienen 5, el número será igual a 10. El problema, entonces, es claro, las relaciones entre los nodos aumentan o crecen más rápidamente que los nodos (a medida que estos van aumentando), lo que puede verse en la figura siguiente.

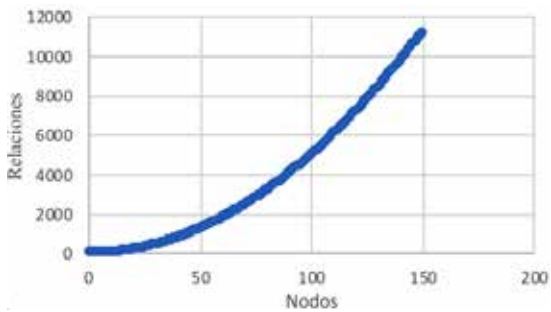


Figura Nº 1: Aumento acelerado del número de relaciones a medida que el número de nodos aumenta.

Fuente: Elaboración propia.

Lo anterior implica que no solo debe verse la estructura en términos de las entidades que la conforman (nodos), sino también, y de manera muy especial, en cuanto a las relaciones que esos nodos determinan y que son los que a la larga van a influenciar la calidad de la respuesta. Una analogía hasta cierto punto adecuada es de una red de pesca. Los nudos de la red representan los nodos y los lazos de cuerda entre cada nudo representa la relación. Una red que tuviera un tejido de seis o siete nodos sería muy fácil de desplegar. Pero una red que tuviera quinientos ya no lo sería tanto. Es cierto que ambas son redes, la pequeña y la grande, y ambas, por tanto, son cualitativamente iguales. Es lo cuantitativo lo que las hace cambiar (la cantidad afecta la calidad), y es esto, en consecuencia, lo que complejiza el empleo y lo que obliga, por ende, a preparar el despliegue con anticipación.

CAPACIDADES MILITARES

El Ejército mantiene organizados sus cuadros a base de estructuras denominadas Tablas de Organización y Equipo (TOEs). Estas tablas son inventarios de personal, material y equipo, y responden —en tanto formaciones de guerra— a una demanda institucional a la que se denomina

4 BARABASI, Albert-Laszlo (octubre 1999). "Emergence of scaling in random", Northeastern University, pp. 509-512. 286(5439):509-12.

"amenaza." Esta amenaza viene representada por uno o varios enemigos potenciales que podrían hacerse efectivos en caso de conflicto. Luego, las TOEs son estructuras pensadas para la guerra, no para situaciones de catástrofes como las que se estudian aquí.

¿Existe en el Ejército un equivalente a las TOEs para casos de catástrofe? La respuesta es que, por el momento, no. Sin embargo, en tanto el Ejército reconozca como a una de sus áreas de misión el apoyo a la emergencia nacional,[5] estará obligado a contemplar el desarrollo de una capacidad de ayuda que se materialice en un órgano o en un conjunto de órganos. No basta con que el Ejército declare poseer un eje de acción, debe además contar con él o los órganos que harán efectiva esa función.

Para efectos del presente estudio, este órgano no contempla una condición añadida a la pre-existente del Ejército, sino que se funda y sobresale a partir de las capacidades actuales.

La capacidad implícita es, para efectos de este estudio, aquella que el Ejército posee y que por sí misma puede emplearse en operaciones distintas a la guerra (MOOTW). Esta capacidad puede tener varios componentes que son directamente reconocibles y que pueden ser intangibles, como la estructura, cadena de mando, protocolos y disciplina; o tangibles, como los comandantes, personal subordinado (hombres y mujeres), vehículos, maquinaria y herramientas, entre otros.

La capacidad implícita es subyacente a las TOEs y, por ende, anterior a ellas. Desde luego, no podría haber estructura en ninguna TOE si no se dieran por existentes estas capacidades implícitas.

Ahora bien, son estas capacidades implícitas las que se trasladan desde la Fuerza Terrestre (FT) hacia el apoyo a la comunidad en casos de catástrofes y emergencias (véase la figura Nº 2).

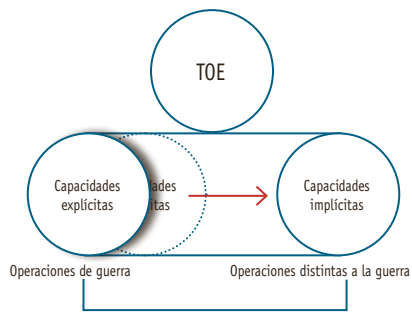


Figura Nº 2: La capacidad implícita subyace a la TOE y es la que contribuye, material y conceptualmente, a enfrentar emergencias y catástrofes.

Fuente: Elaboración propia.

5 Ejercito de Chile, El Ejército. Santiago, Chile, División Doctrina, 2017. DD-10001.

CAPACIDADES MILITARES EN EMERGENCIA

Una capacidad militar, por otra parte, es (además de lo ya dicho) una relación que se da entre un determinado medio, organismo o equipo, y el empleo que se hará de él. Un equipo, por sí solo, no puede representar una capacidad porque se encuentra regulado y sometido al escenario en el que deberá actuar; a las capacidades propias para operar ese equipo; a las capacidades de los otros equipos que lo acompañan, ya sea para transportarlo, mantenerlo o abastecerlo; y no menos que a las capacidades de la amenaza a la que se enfrenta, pues la capacidad del enemigo también influye en la capacidad propia. Así, las capacidades no se dan en el vacío (es decir, con respecto a sí mismas), sino con respecto a otras cosas. Esta interacción profunda entre lo que la capacidad se dice que es y lo que se espera de ella, dado todo el conjunto que forma el entorno de la misma, es lo que definimos como tal.

En consecuencia, tomando en cuenta esta definición y trasladando su realidad al contexto de las emergencias producidas por las catástrofes, ya sea naturales o causadas por el hombre, tenemos que la capacidad es aquel conjunto de medios materiales y humanos en condiciones de enfrentar una amenaza (el incendio de un bosque, por ejemplo) con una fuerza, en un momento, y con acciones que resulten oportunas.

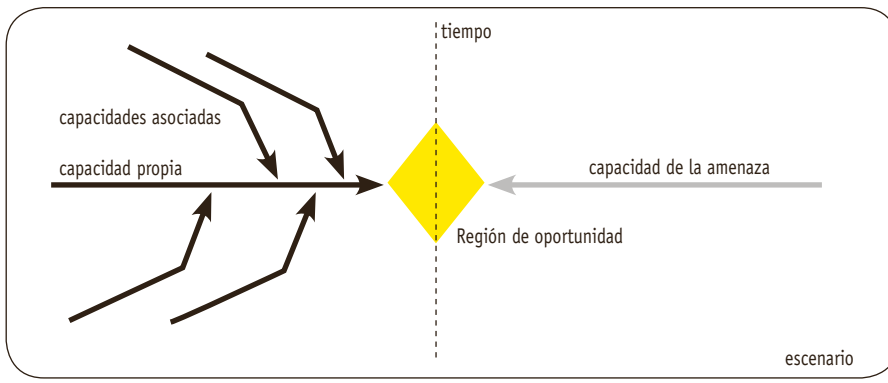


Figura N.º 3: Diagrama que muestra la capacidad propia en función de la amenaza y de las capacidades asociadas en un escenario dado.

Fuente: Elaboración propia.

INTERFACES DEL EJÉRCITO Y EL SISTEMA NACIONAL DE PROTECCIÓN CIVIL

De lo revisado anteriormente, se desprende que el Ejército cuenta con una capacidad para enfrentar operaciones distintas a la guerra, que le permite prestar ayuda humanitaria a la comunidad en situaciones de emergencias y catástrofes. Esta ayuda, no obstante, no se presta en cualquier circunstancia y se encuentra sujeta, por tanto, a diversos límites y procedimientos establecidos por la autoridad de gobierno, que es la encargada de llevar adelante la acción del aparato público en auxilio de los más necesitados.

Para lo anterior, lo primero que se debe entender es que el Ejército no es el organismo encargado de articular la ayuda, este organismo es el Ministerio del Interior, el cual a su vez opera por medio de una oficina especializada llamada ONEMI. Esta última no posee, en la práctica, medios propios para actuar, por el contrario, su fortaleza radica en la información con que cuenta y en los procedimientos con que opera, además de su sistema de información distribuido a lo largo del país. Esta mezcla de información y procedimientos es lo que le permite a la ONEMI coordinar la ayuda, de tal manera de canalizarla por el camino más corto hacia quien la necesita.

Esta configuración, en cierto modo asimilable a un hub informático, permite, por una parte, concentrar la capacidad de ayuda y, por otra, distribuirla. Concentrar las capacidades en un solo ente que, a su vez, se encuentra descentralizado en oficinas regionales, permite en teoría llevar la acción de rescate con toda la fuerza y autoridad del Estado, y plasmarla justo allí donde se requiere. Para conseguirlo, se vale de un marco legal y de medios que ejecutan aquel marco, uno de los cuales es el Ejército. El marco legal en cuestión se halla configurado de tal manera que permite responder en escala según la gravedad de la situación de crisis, esto es, concede a la autoridad política la posibilidad de dotar de mayores atribuciones a los encargados de organizar el socorro en las zonas más afectadas. Así, es posible que colinden dos zonas con regímenes constitucionales distintos, sin que ello implique conflicto alguno.

MODELO PROPUESTO

Un modelo es un producto de la imaginación. Como tal, los modelos se extraen, a su vez, de los sistemas que son estructuras igualmente imaginarias, aunque con un componente de realidad que normalmente se halla representado por los nodos de la misma. Es el caso de la ONEMI, la CONAF, el Ejército, la Armada, entre otros. Estos nodos se relacionan entre ellos mediante acuerdos que reciben el nombre de protocolos, convenios, órdenes, regulaciones, etcétera. Este conjunto, en definitiva, de nodos y relaciones más o menos conceptuales se pueden visualizar mediante modelos. Los modelos pueden ser de los tipos más variados, y van desde los procesos hasta los organigramas, pasando por cualquier clase de declaración esquemática o narrativa que se refiera a asuntos del mundo real.

El modelo que este trabajo propone no es, por tanto, el modelo de solución al problema de facilitar al mando institucional la toma de decisiones en situaciones de emergencias y catástrofes, sino un modelo que con el tiempo puede ir variando o completándose a medida que vaya ganando en experiencias.

Al modelo que aquí se presenta se le ha denominado de asignación de recursos. Este modelo de asignación o módulo de asignación es una herramienta que le permite a la autoridad decidir sin tener que pensar mayormente en detalles subsidiarios.

Para ello, él mismo toma en cuenta el tipo de emergencia que se haya producido y lo compara con los tipos de unidades con que se cuenta para enfrentar estas emergencias (ver figura siguiente).

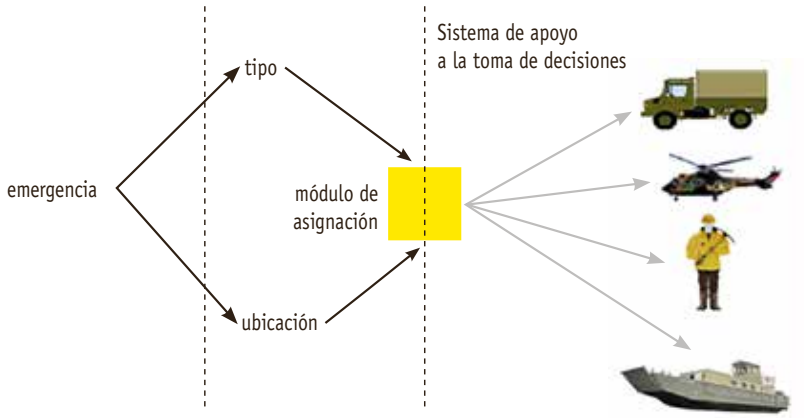


Figura Nº 4: Módulo de asignación del modelo de apoyo a la toma de decisiones.

Fuente: Elaboración propia.

Como se puede ver, el modelo o módulo de asignación del modelo es una herramienta muy simple pero que puede resultar de gran utilidad, en la medida que cuente con datos actualizados y reales, facilitando no solo la toma de decisiones de manera más rápida, sino que registrando además todo lo resuelto, el número y tipo de unidades empleadas, y, eventualmente, el rendimiento que haya tenido cada una en la fase de ejecución de las tareas. En virtud de lo anterior, los requerimientos de alto nivel para la aplicación fueron los siguientes:

- Debe permitir a la autoridad conocer la ubicación y disponibilidad en tiempo real de las capacidades o recursos militares que se pueden utilizar para combatir una catástrofe nacional del tipo que fuere.
- Debe funcionar y ejecutarse en un servidor web, que permita a los diferentes usuarios conectarse vía intranet de manera remota, utilizando protocolos de seguridad adecuados a la información que se manejará.

Debe tener una arquitectura informática con los siguientes componentes:

- Módulo de Base de Datos: este módulo es el encargado de almacenar los datos relacionados con las capacidades o recursos militares disponibles en las unidades, junto con los datos de autenticación de los usuarios. Debe permitir también la comunicación de datos entre el módulo "Interfaz Web" y el módulo "Cálculo de Soluciones". La programación de este módulo puede ser realizada mediante el sistema de gestión de base de datos MySQL (software libre) o SQLServer.
- Módulo Interfaz Web: este módulo es el encargado de la autenticación de los usuarios mediante un nombre, una clave y un procedimiento extra de autenticación. Debe permitir

además el ingreso de datos que el usuario entregue al sistema y desplegar los resultados de la asignación "Cálculo de Soluciones." Este módulo puede programarse en un lenguaje para interfases web tales como HTML, Java Script y componentes de PHP; este último debe incorporarse debido al flujo dinámico de datos de la aplicación (interno) y la comunicación que debe tener con la base de datos (externo).

- Módulo de Asignación: este módulo es el encargado de la implementación de los algoritmos o heurísticas que permiten determinar la planificación y operación de un sistema de asignación de capacidades militares, en condiciones de ser empleadas en una catástrofe o emergencia nacional. Esta aplicación debe permitir la asignación en tiempo real de las capacidades de acuerdo a la distancia a la que las unidades se encuentren de la emergencia, para lo cual debe ser programada en forma georreferenciada. Este módulo es el motor y núcleo del sistema, ya que por medio de su implementación es posible obtener los resultados que el usuario requiere. Se comunica directamente con la base de datos, obteniendo el valor de las variables involucradas en el modelo a resolver para luego almacenar los resultados de la solución, los que serán posteriormente leídos por el módulo Interfaz para la visualización al usuario. Este módulo debe ser implementado de la manera más eficiente posible, debido a que es el que entrega los resultados, particularmente cuando debe hacerlo en tiempo real; por esta razón, se pretende programar este módulo mediante técnicas de multiprocesamiento, con librerías de optimización, que son las que permiten trabajar de forma paralela, reduciendo notoriamente el tiempo de cómputo. La programación de este módulo puede ser realizada en un lenguaje de bajo nivel como C o C++. La estructura principal del sistema se emplea y focaliza principalmente en disminuir la transmisión de datos entre los módulos. Finalmente, el módulo de Cálculo de Soluciones adquiere la información de la base de datos, resuelve el modelo de optimización seleccionado y almacena la solución, la cual será leída por el módulo Interfaz Web, que la entregará al usuario.

Debe poseer las siguientes características generales:

- Facilidad de uso: la aplicación debe ser de uso fácil y directo para el usuario. La característica principal de esta propiedad reside en el contenido del módulo Interfaz Web, el cual debe ser de baja navegabilidad, de rápido acceso y amigable.
- Independencia: los módulos del sistema deben estar estructurados de forma independiente, de manera de asegurar que la eventual falla de uno no implique la falla de los restantes.
- Eficiencia: según lo descrito en el módulo de Cálculo de Soluciones.
- Georreferencia: según lo descrito en el módulo de Cálculo de Soluciones.
- Acceso remoto y ubicuidad: según lo descrito en los módulos Base de Datos e Interfaz Web.
- Acceso remoto y seguro: según lo descrito en el Módulo Base de Datos.
- Base de Datos.

A continuación, se presenta el diagrama que representa todo el proceso que va desde el ingreso a la aplicación y la visualización de la emergencia, hasta el módulo de evaluación final.

En él se puede apreciar la trama que va desde la autenticación del usuario, pasando por la carga de la emergencia, la propuesta de asignación de recursos, y las modificaciones que la autoridad desee incorporar, hasta la evaluación del rendimiento de los recursos asignados.

A partir del momento en que la autoridad decide optar por un determinado conjunto de unidades, el sistema ejecuta la decisión que llega en forma de orden a él o a los comandantes encargados de materializarlas.

En la siguiente figura se describe el diagrama de flujo de la base de datos de la aplicación.

Ahora bien, nada de esto es visible para el operador, lo que se muestra aquí es la secuencia de pasos que encaminan el proceso desde el problema a la solución.

El operador —en este caso, la autoridad— ve un mapa, y sobre ese mapa va completando mediante clics digitales su decisión. Esos clics los hace directamente sobre la interfaz gráfica.

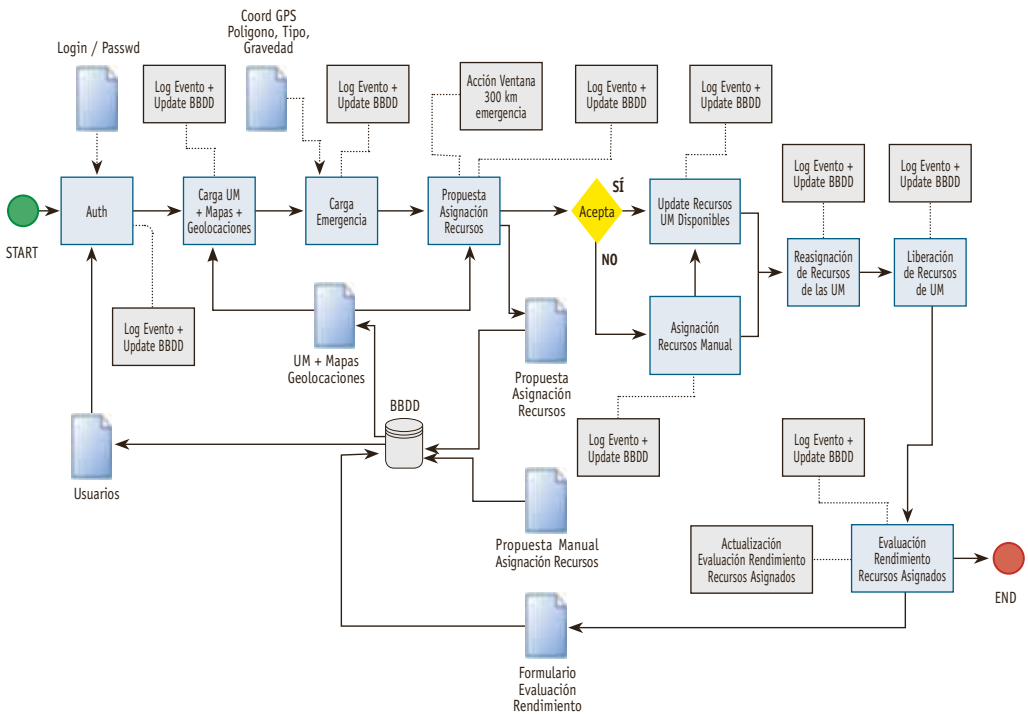


Figura Nº 5: Módulo de Base de Datos de la plataforma propuesta.

Fuente: Elaboración propia.

PLATAFORMA

Finalmente, el modelo matemático antes descrito y el modelo de base de datos son ingresados en un Sistema de Información Geográfico gratuito de carácter colaborativo llamado "Gis Cloud", donde se comunican los cientos de usuarios mediante una aplicación móvil con un administrador web con acceso al panel de control del sistema de control.

La siguiente imagen explica la arquitectura de este sistema de información geográfica en la nube, abajo a la izquierda se señala "Work Management". En esa función fue desarrollada nuestra aplicación.

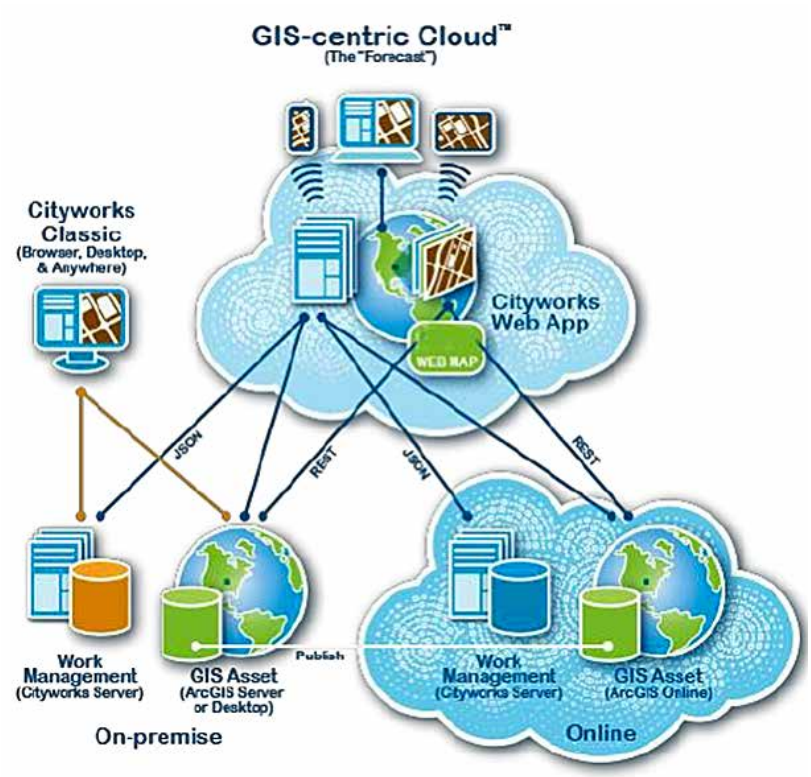


Figura Nº 6: Módulo de Base de Datos de la plataforma propuesta.

Fuente: PURWONEGORO, Berni "Cloud Computing Concept", Badan Informasi Geospatial p. 5, mayo 2015. 7774 TS 1A – Standards, 7553.

Lo anterior es un sistema *per se* y, a la vez, un sistema de entrenamiento.

Un sistema debido a que tiene la capacidad de utilizarse en tiempos reales para el control y conducción de unidades civiles y militares. Y un sistema de entrenamiento, ya que puede generarse eventos simulados para entrenar la capacidad de un comandante o autoridad en la toma de decisiones.

Esta plataforma además fue *customatizada* para generar mayor realismo a la autoridad militar y poseer el mismo lenguaje militar de los usuarios, como lo muestra la siguiente figura:

Figura Nº 7: Plataforma web.

Fuente: Elaboración propia.

Finalmente, se utilizó la aplicación móvil por parte de Gis Cloud para el envío de datos, como se indica en la siguiente figura:

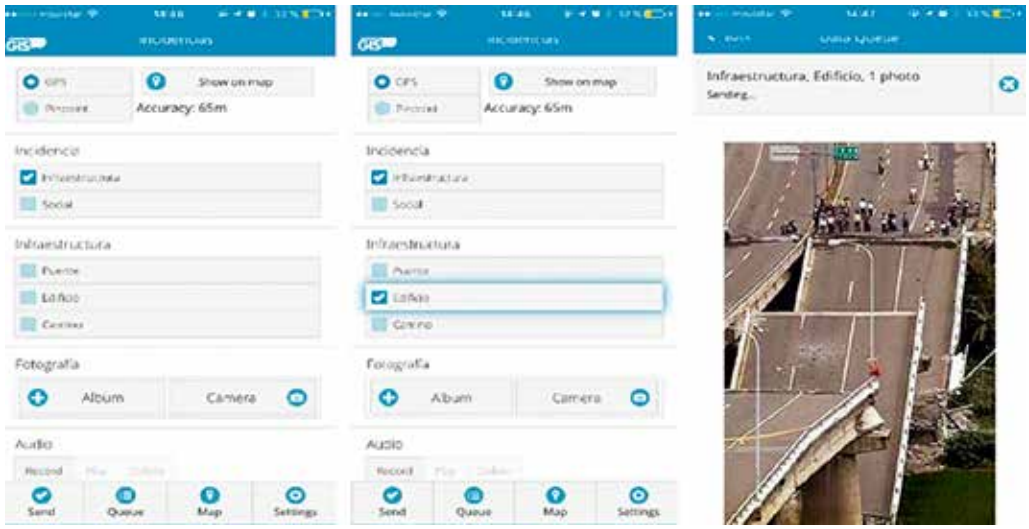


Figura Nº 8: Aplicación móvil en tres instancias para el envío de información.

Fuente: Elaboración propia.

CONCLUSIONES

Hasta el terremoto de febrero de 2010, el Ejército, que es parte importante del sistema de respuesta de la autoridad a emergencias o catástrofes, no contaba con una estructura diseñada para el tipo de demandas que estas situaciones plantean. Aun así, contaba con capacidades preexistentes que tienen que ver con su estructura, su régimen jerárquico y de disciplina, su mapa de relaciones funcionales, entre otras. Estas capacidades le permiten readecuar, con las capacitaciones y medios adecuados, su orgánica, y prestar servicios como los que demandan las situaciones de riesgo de origen natural, sean estas causadas o no por el hombre.

Ahora bien, efectivamente el Ejército diseñó una estructura de respuesta a emergencias no solo en la planificación o la coordinación, sino que especialmente en los medios encargados de materializar la acción. Esta estructura integral (i.e., planificación y medios efectivos) es la que enfrenta las necesidades de la ciudadanía, canalizadas por el Ministerio del Interior a través de la ONEMI. Dicho de otro modo, no es todo el Ejército el que se emplea, sino aquella parte de él que ha sido designada para emplearse. Ello implica que las unidades en cuestión tienen o cumplen una función dual, no específica o excluyente, de modo que una unidad con misiones para enfrentar incendios sigue siendo esencialmente una unidad preparada para el combate terrestre.

El Centro de Modelación y Simulación del Ejército, por su parte, tomando como base esta realidad, y las experiencias dejadas por las emergencias y catástrofes recientes sufridas por una parte importante de la población, diseñó una aplicación que permite relacionar la estructura establecida por el Ejército para enfrentar catástrofes con las necesidades que ellas van generando, y que se presentan en formas de requerimientos muy difíciles de predecir.

Esta aplicación se encuentra en fase de estudio preliminar, pero todo su perfil y prestaciones se encuentran definidos. Es una herramienta fácil de usar y su filosofía reside en un esquema que une el problema (una necesidad dada de la población) con la solución (una capacidad del sistema de respuesta institucional), en un tiempo mínimo. Para ello se ha diseñado un sistema de acceso rápido que no solo muestra la situación que se está viviendo, sino que además ofrece las opciones más inmediatas a la autoridad.

Se espera, en los próximos meses, consolidar el piloto de la aplicación y validarlo en los distintos niveles que participan en el sistema de respuesta a catástrofes. Con el tiempo, la aplicación debiera estar repartida en todos los organismos involucrados, facilitando con ello la acción, disminuyendo los tiempos de respuesta, y asegurando la oportunidad en la ayuda o el apoyo a la comunidad.

BIBLIOGRAFÍA

BARABASI, Albert-Laszlo. "Emergence of scaling in random", Northeastern University, pp. 509-512, octubre de 1999. 286(5439):509-12.

Centro de Lecciones Aprendidas (2017). El empleo de la Fuerza Terrestre en la operación 27F, Santiago, Chile, División Doctrina, p. 9.

Ejército de Chile (2017). El Ejército, Santiago, Chile, División Doctrina. DD-10001.

PURWONEGORO, Berni. "Cloud Computing Concept", Badan Informasi Geospatial p. 5, mayo 2015. 7774 TS 1A – Standards, 7553.

APOYO DE LAS OPERACIONES CIBER-ELECTROMAGNÉTICAS A LA FUERZA TERRESTRE[1]

MAYOR OSVALDO ALANIZ MIRANDA[2]

Resumen: *el ciberespacio constituye una nueva dimensión en el campo de batalla, la cual ha revolucionado el paradigma existente respecto al empleo de fuerzas militares en los conflictos modernos. En la actualidad, la OTAN está desarrollando el concepto de las Actividades Ciber-electromagnéticas o CEMA (Cyber Electromagnetic Activities), las cuales constituyen un nuevo paradigma de capacidad militar[3] basado en la integración de las operaciones de guerra electrónica y las ciberoperaciones en forma coordinada, debido principalmente a que el ciberespacio y el espectro electromagnético se encuentran totalmente fusionados e integrados en una gran dimensión a nivel físico y lógico. El presente artículo propone la integración de las operaciones ciber-electromagnéticas en apoyo a las unidades de la Fuerza Terrestre, con el propósito de obtener la libertad de acción en el ciberespacio y en el espectro electromagnético, mediante la aplicación de medidas defensivas y ofensivas en dichas dimensiones en apoyo a las operaciones militares durante crisis, EPB[4] y MOOTW.*[5]
Palabras clave: *ciberoperaciones, espectro electromagnético, ciberespacio, guerra electrónica, actividades ciber-electromagnéticas (CEMA).*

Abstract: *cyberspace is a new dimension within the battlefield, which have revolutionized the paradigm prevalent in relation to the use of military forces in the modern conflicts. Nowadays, NATO is developing a concept called Cyber electromagnetic Activities (CEMA). Which constitute a new military capability paradigm, based on the integration and coordination of Electronic Warfare Operations and Cyber space operations, because of cybersapce am electromagnetic spectrum, are totally merged and integrated in a big physical and logical dimension. This article, propose the integration of Cyber electromagnetic*

1 Artículo ganador del segundo puesto del concurso "Desarrollando Capacidades Militares", en el ámbito de Ciencias Militares, Combate, Generación de Doctrina y Docencia

2 Oficial de Ejército, especialista de Estado Mayor, profesor de academia en Historia Militar y Estrategia, magíster en Educación Superior de la Universidad Andrés Bello.

3 Capacidad militar es el conjunto de diversos factores (sistemas de mando y control, sistemas de armas, entrenamiento, infraestructura, personal y medios de apoyo logístico) establecidos sobre la base de principios y procedimientos doctrinarios que pretenden conseguir un determinado efecto militar a nivel estratégico, operacional o táctico para cumplir las misiones asignadas. (RAA-03008 Proceso de Desarrollo de Capacidades Militares, edición 2013, p. 22)

4 Empleo del potencial bélico.

5 Operaciones militares diferentes a la guerra.

operations supporting the ground forces in order to gain freedom of action in both cyberspace and electromagnetic spectrum, through the aplication of defensive and offensive measures in both dimensions by supporting military operations during periods of crisis, war and military operations other tan war.
Keywords: *cyberoperations, electromagnetic spectrum, electronic warfare, cyber electromagnetic activities (CEMA).*

INTRODUCCIÓN

Los últimos conflictos han demostrado la importancia de la integración de la guerra electrónica y las ciberoperaciones en apoyo a fuerzas convencionales e incluso su explotación por parte de fuerzas insurgentes con el propósito de ganar la iniciativa y la libertad de acción en el espectro electromagnético y en el ciberespacio. Las lecciones aprendidas obtenidas por los rusos en la campaña en Georgia y Osetia del sur el año 2008 determinaron sus deficiencias en la integración de diferentes redes de telecomunicaciones, la incapacidad de neutralizar la amenaza de radares de las fuerzas georgianas, la necesidad de Unmanned Aereal Vehicle (UAV) como medios de obtención y la falta de apoyo de operaciones de guerra electrónica y ciberoperaciones a las fuerzas convencionales.[6] Dichas lecciones aprendidas serían totalmente aplicadas durante las operaciones de los rusos en Ucrania y el conflicto en Siria, en donde pusieron en práctica la "Doctrina Gerasimov" o "Guerra no lineal",[7] la cual busca paralizar, destruir y neutralizar el proceso de toma de decisiones del adversario mediante la combinación del empleo de fuerzas convencionales y unidades irregulares con el apoyo de operaciones de guerra electrónica y ciberoperaciones. A modo de ejemplo, en 2015, durante la campaña en Crimea, los rusos realizaron ciberataques[8] contra dos empresas de electricidad en Ucrania, dejando sin energía eléctrica a 80.000 hogares. Asimismo, afectaron la infraestructura crítica de telecomunicaciones e Internet en la península de Crimea, lo cual causó severos daños en los servicios de telefonía celular, enlaces de radio y páginas web del gobierno ucraniano.

En el contexto nacional, la Fuerza Terrestre no se encuentra ajena a esta realidad por cuanto gran parte de los sistemas de armas y los diferentes sistemas de mando y control (C2) emplean el ciberespacio y el espectro electromagnético como medios de transmisión de altos volúmenes de información digital y grandes anchos de banda que permiten conducir las operaciones con el propósito de obtener un ciclo OODA[9] superior al adversario, así como la superioridad en la información

6 Ministry of Defense, Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities, Chief of Staff, febrero de 2018, p. 7.

7 Es una estrategia militar que combina el empleo de fuerzas convencionales, fuerzas irregulares, operaciones de guerra electrónica y ciberoperaciones, combinando acciones kinéticas con acciones subversivas en las cuales el agresor buscará evadir su responsabilidad como autor. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimovdoctrine-and-russian- on-linear-war/

8 Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan. FOXALL, P. "Putin´sCyberwar: Rusia´s Statecraft in the Fifth Domain", *Russia Studies Centre,* Policy Paper N°16, May 2016.

9 Ciclo de Boyd: observar, orientar, decidir y actuar.

mediante el despliegue del sistema Command, Control, Comunications, Computers, Intelligence, Surveillance, Target Acquisition and Reconnaissance (C4ISTAR) a nivel brigada y división.

MARCO DOCTRINARIO Y JURÍDICO

Desde la perspectiva doctrinaria, las Ciberoperaciones[10] y la Guerra Electrónica[11] (EW) se encuentran insertas en la planificación y ejecución de las Operaciones de Información (INFOOPS), Guerra de Mando y Control (C2W), como medios de obtención de inteligencia y mediante el empleo de multiplicadores de combate a través de fuegos no letales en coordinación con el Centro de Apoyo de Combate (CAC) del Cuartel General de la Unidad de Armas Combinadas en el nivel táctico de las operaciones. Respecto a la ciberdefensa, responde y acciona sobre alertas, amenazas y ataques contra el sistema de Comando, Control, Comunicaciones y Computación (C4), y aprovecha la inteligencia, contrainteligencia y operaciones especiales de espionaje y sabotaje cuando sea necesario.

Desde la perspectiva jurídica, las ciberoperaciones y la EW (SIGINT),[12] se encuentran amparadas en la Ley N° 19.974 "Sobre el sistema de inteligencia y crea la Agencia Nacional de Inteligencia", conforme a lo cual las unidades ejecutivas de ciberoperaciones y de EW se encuentran encuadradas en la Dirección de Inteligencia del Ejército (DINE).[13]

CIBERESPACIO Y ESPECTRO ELECTROMAGNÉTICO: VARIABLES INTANGIBLES DEL CAMPO DE BATALLA

ESPECTRO ELECTROMAGNÉTICO

Corresponde a una variable del campo de batalla, compuesta a base de un conjunto ordenado de frecuencias de ondas electromagnéticas, que considera todas aquellas que pueden ser irradiadas, transmitidas, recibidas y/o simuladas por dispositivos electrónicos. Este recurso es ampliamente utilizado en las operaciones militares por los equipos de comunicaciones para el transporte de información e integración de los sistemas de mando y control, por los sensores asociados con sistemas de armas para la detección de blancos, así como para degradar las comunicaciones del adversario.

---

10 Según la doctrina de ciberdefensa del Ejército de Chile, las ciberoperaciones se dividen en ciberoperaciones defensivas y en ciberoperaciones ofensivas. RDI-20008, Reglamento Ciberdefensa, 2016.

11 Comprende el conjunto de actividades a través de las cuales se pretende asegurar sobre el adversario, la superioridad en el empleo del espectro electromagnético en aquellas zonas del campo de batalla, que en cada caso se considere de interés, y asegurar su empleo eficaz por las fuerzas propias. Para ello, se orienta en dos actividades fundamentales. La primera es la inteligencia de señales, relacionada con la función inteligencia y con la ubicación de estaciones de radio y radares. La segunda es la actividad de operaciones de guerra electrónica, vinculada a la función de combate de maniobra.

12 Signal Intelligence, la cual se divide en COMINT (Inteligencia de Comunicaciones) y ELINT (Inteligencia Electrónica).

13 Específicamente, el RINTE N°2 "Llaitún" cuenta con un batallón de Ciberdefensa y un batallón de EW organizados por TOE. Asimismo, las Agrupaciones de Inteligencia (AGRINTs) cuentan en su orgánica con pelotones SIGSEC (Seguridad de Señales) y pelotones y compañías de Operaciones de EW, como es el caso del pelotón COMINT "Caliche" y la Compañía EWOPS "Huara".

De este modo, el espectro electromagnético es el ámbito de actuación de la guerra electrónica que abarca desde las frecuencias que utilizan las telecomunicaciones por radio de los submarinos a larga distancia, pasando por las bandas de radiodifusión, enlaces tácticos, cable herciano (CBH), televisión, radar, enlace con satélites, radiación infrarroja, espectro óptico de la luz visible (del rojo al violeta), hasta la radiación ultravioleta, los rayos X, las radiaciones gamma y los rayos cósmicos.

En la actualidad, todos los sistemas de telecomunicaciones, radares aéreos y terrestres, sistemas C4ISR, comunicaciones satelitales, internet inalámbrico, sistemas GPS, tráfico aéreo, radioemisoras FM, AM, radioaficionados y casi la totalidad de las aplicaciones militares y civiles emplean el espectro electromagnético para transmitir y recibir información a largas distancias. A nivel mundial, su gestión y administración es realizada por la International Telecomunication Union (ITU), organismo especializado de Naciones Unidas para las Tecnologías de la Información y la Comunicación –TIC. En tanto, a nivel nacional, el espectro electromagnético es administrado por el Ministerio de Transportes y Telecomunicaciones a través de la Subsecretaría de Telecomunicaciones de Chile (SUBTEL) y conforme a la Ley General de Telecomunicaciones.[14]

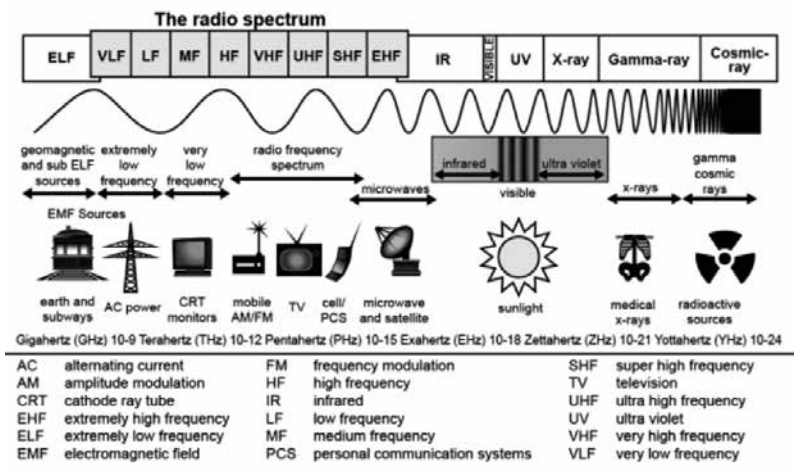


Figura N° 1: El espectro electromagnético.

Fuente: US ARMY, TRADOC FM 3-38 "Cyber Electromagnetic Activities".

EL CIBERESPACIO

El ciberespacio corresponde a una variable del campo de batalla, además de ser un dominio dentro del ambiente de la información que consiste en las redes interdependientes de tecnologías de la información, infraestructura y datos, incluyendo Internet, redes de telecomunicaciones, sistemas computacionales y procesadores, así como sistemas de telefonía celular, sitios web e infraestructura técnica de redes y

14 República de Chile, Ley General de Telecomunicaciones N°18.168 del 2 de octubre de 1982.

comunicaciones.[15] Según la doctrina nacional es un espacio virtual que contiene los sistemas de redes informáticas, los que utilizan medios físicos y el espectro electromagnético para interconectarse y realizar las funciones de procesamiento, almacenamiento y difusión de la información requerida por el sistema de mando y control; su dominio puede llegar a constituir un factor multiplicador de la fuerza.

El ciberespacio consta de una capa física, una capa lógica y una capa de cyber-persona, en la cual la primera corresponde a la infraestructura física, hardware, redes LAN, fibra óptica, routers, switches, hubs y terminales computacionales. La capa lógica son aquellos elementos de la red que están relacionados entre sí de una manera que se abstraen de la red física, es decir, la forma o las relaciones no están vinculadas a un individuo, una ruta o nodo. La capa ciber-persona es una representación digital de una identidad real o la creación de diferentes identidades ficticias en el ciberespacio; una persona real puede incorporar algunos datos biográficos o corporativos, correo electrónico, dirección IP, número telefónico, etc., sin embargo, esta persona también puede crear diferentes identidades o usuarios falsos.

Respecto a la realidad del Ejército de Chile, cabe hacer mención que casi la totalidad de los sistemas de armas, sistema de inteligencia y plataforma tecnológica de mando y control (C2), emplean el espectro electromagnético y el ciberespacio como medios de transmisión y recepción de grandes volúmenes de información, los cuales están asociados a medios ISR, apoyo de fuego, Panorama Operacional Común (POC), radares, sistemas de guerra electrónica (EW), comunicaciones satelitales, sistemas de gestión logística y documental entre otros, los cuales, de ser degradados, podrían afectar seriamente la conducción de la Fuerza Terrestre tanto en crisis como en EPB.

Conforme a lo anterior, la gestión, administración y protección del espectro electromagnético y del ciberespacio de la Fuerza Terrestre es una tarea fundamental.

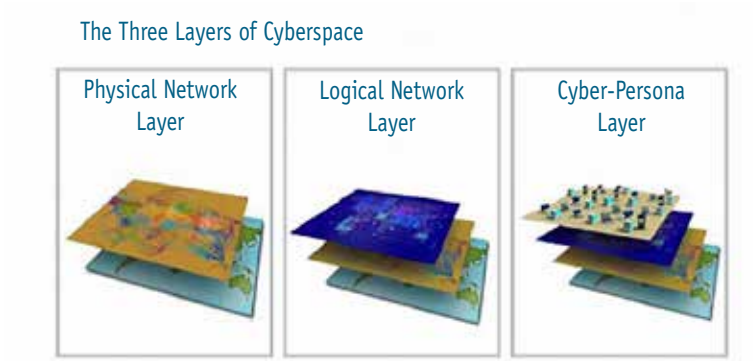


Figura N° 2: Las tres capas que componen el ciberespacio.
Fuente: JP 3-12 Cyberspace Operations. Joint Chief os Staff, 2018.

15 FM 3-12 "Cyberspace and ElectronicWarfare Operations", Headquarters Department of the Army, April 2017, p. 1-2.

TENDENCIA MUNDIAL

En la actualidad, y a nivel mundial, la amenaza convencional y no convencional está desarrollando capacidades ofensivas en el ciberespacio, tales como malwares, drones de bajo costo[16] e incluso armamento anti-satélites diseñados para degradar los sistemas de mando y control (C2) y Tecnologías de la Información y las Comunicaciones (TICs), los cuales permiten conducir las operaciones, así como mantener la libertad de acción en el ciberespacio y en el espectro electromagnético.

Asimismo, las nuevas amenazas cuentan con tecnología de bajo costo y capacidades para realizar acciones ofensivas en el ciberespacio mediante acciones de OSMO (Offensive Social Media Operations) empleando redes sociales y medios de difusión masiva para realizar Operaciones Psicológicas[17] y desinformación sobre un público objetivo determinado.

Durante el conflicto en Ucrania, los hackers rusos (Grupo Fancy Bear) insertaron malwares en los sistemas operativos Android de las unidades de artillería del Ejército ucraniano, lo cual permitió a las fuerzas rusas conocer la ubicación exacta de dichas unidades en el terreno para posteriormente degradarlas mediante acciones directas.

Posteriormente, durante las maniobras de la OTAN en Estonia en abril de 2017, en la cual participó un contingente de 4.000 hombres del Ejército de EUA, se detectaron operaciones ciberofensivas por parte de fuerzas rusas mediante el hackeo de los smartphones de las tropas de la Alianza Atlántica, borrando sus contactos telefónicos e insertando música que nunca habían bajado de internet, lo cual obligó a los mandos a disponer la prohibición de usar dichos aparatos así como retirar las tarjetas SIM de todos los celulares.

Más recientemente, EUA ejecutó ciberoperaciones ofensivas[18] (OCO) en contra de ISIS, las que fueron llevadas a cabo por la Fuerza de Tareas Conjunta Ares, la cual se concentró en destruir y desorganizar las redes de computadores usados por los islamistas para reclutar guerrilleros y también para establecer la plataforma tecnológica de dicho grupo.

Asimismo, esta campaña tuvo como esfuerzo principal la degradación del sistema de propaganda en Internet, accediendo a las cuentas en redes sociales de los miembros de ISIS, logrando

16 El 6 de enero de 2018, un grupo de 13 drones de bajo costo del grupo ISIS atacó la base aérea rusa de Hmeymim y la base naval de Tartus. Los rusos lograron derribar 7 drones con misiles antiaéreos de alto costo, además de capturar el resto gracias a medios de EW que lograron neutralizarlos. ("*Russia says it killed rebels behind swarm drone attack in Syria, but experts see more such strikes ahead*". Published 7:17 PM ET Fri, 12 Jan 2018CNBC.com Kirill Kudryavtsev.

17 Según la OTAN y la doctrina de EUA, las PsyOps han pasado a denominarse MISO (Military Information Support Operations) y forman parte de las INFOOPS.

18 Conforme la doctrina CEMA de EUA, se pueden obtener diferentes efectos "no kinéticos" en beneficio de la maniobra a nivel táctico y operacional sobre nodos críticos de mando y control, así como sobre infraestructura crítica de las TICs de la amenaza conforme a lo siguiente: degradar, denegar, destruir, engañar, manipular, perturbar, desorganizar y neutralizar.

cambiar sus claves de acceso, además de borrar videos propagandísticos y de acciones de combate del Estado Islámico desde Internet.[19]

LAS ACTIVIDADES CIBER-ELECTROMAGNÉTICAS (CEMA)

Las actividades ciber-electromagnéticas (CEMA) corresponden a las actividades y operaciones destinadas a capturar, retener y explotar las ventajas sobre el adversario en el ciberespacio y en el espectro electromagnético, así como denegar y degradar al adversario el uso del mismo y, finalmente, proteger el sistema de mando y control propio.[20] CEMA consiste en operaciones en el ciberespacio (CO), guerra electrónica (EW) y operaciones de administración del espectro (SMO). En síntesis, el propósito de este nuevo concepto es asegurar la libertad de acción en el ciberespacio y en el espectro electromagnético, obtener la superioridad en la información en dichas dimensiones, así como alcanzar un ciclo OODA (observar, orientar, decidir y actuar) superior al adversario.

Las actividades ciber-electromagnéticas (ACEM) son responsabilidad de todo comandante y de su respectivo estado mayor, debiendo ser integradas y sincronizadas en todos los niveles de mando y funciones de combate. Los comandantes, apoyados por su estado mayor, integran las ciberoperaciones, las operaciones de espectro electromagnético y operaciones de guerra electrónica en forma conjunta. El Equipo de Trabajo de Guerra Electrónica[21] es el responsable de coordinar las tareas de ACEM, las cuales pueden incluir Inteligencia de Señales (SIGINT) y Operaciones en Red (NETOPS).[22] Las ACEM son una fusión entre las operaciones que se desarrollan con el propósito de obtener la superioridad en el espectro electromagnético y en el ciberespacio, obteniendo con ello libertad de acción, iniciativa y libertad de maniobra sobre el adversario.

Este concepto está siendo desarrollado por la OTAN a través del Joint Concept Note (JCN) 1/17, Future Force Concept, en el cual se determinó la necesidad de integrar las ciberoperaciones y la guerra electrónica producto del éxito de este tipo de operaciones por parte del Ejército ruso en el conflicto con Ucrania, en el cual se sincronizaron y coordinaron acciones ofensivas contra la infraestructura crítica de mando y control en beneficio del accionar de las fuerzas convencionales.[23] Asimismo, se ha evidenciado que la superioridad tecnológica está siendo amenazada por TTPs[24] de guerra no-convencional mediante el empleo de actividades ciber-electromagnéticas (CEMA), como, por ejemplo, el uso de drones como plataformas de ISR y como vectores de ataque por parte de fuerzas insurgentes del ISIS.

---

19 LAMOTHE, Dan (2017). "How the Pentagom´s Cyber Offensive against ISIS could shape the future for elite US forces". The Washington Post.
20 FM 3-36 "Cyber Electromagnetic Activities", Department of the Army, 2016.
21 CEMA Working Group, equipo liderado por el oficial de Guerra Electrónica (EWO) del cuartel general y conformado por oficiales de Inteligencia, Operaciones, Telecomunicaciones, Fuegos y Asesor Jurídico, entre otros.
22 ADRP 6-0 "Mission Command", Headquarters Department of the Army, May 2016.
23 MINISTRY of Defense, Joint Doctrine Note 1/18 *Cyber and Electromagnetic Activities*, Chief of Staff, febrero de 2018, p. 25.
24 Tácticas, técnicas y procedimientos.

En la actualidad, el Ejército de EUA, mediante su programa "CEMA Support to Corps and Below", se encuentra en un proceso de experimentación en cuanto al apoyo de operaciones ciber-electromagnéticas a nivel táctico a nivel de BCTs[25] (Equipos de Combate de Brigada), mediante el apoyo directo de equipos especialistas en guerra electrónica y ciberoperaciones con la misión de realizar tareas de SIGINT, Ataque Electrónico[26] y acciones ofensivas y defensivas en el ciberespacio y en el espectro electromagnético.

En este contexto, el Ejército de EUA ha puesto en marcha el concepto CEMA a través de la creación del Military Intelligence Ranger Battalion, el cual cuenta en su orgánica con una Compañía CEMA, en la que se integra y sincronizan tareas de ISR explotando el ciberespacio y el espectro electromagnético a base de equipos de guerra electrónica y ciberoperaciones.

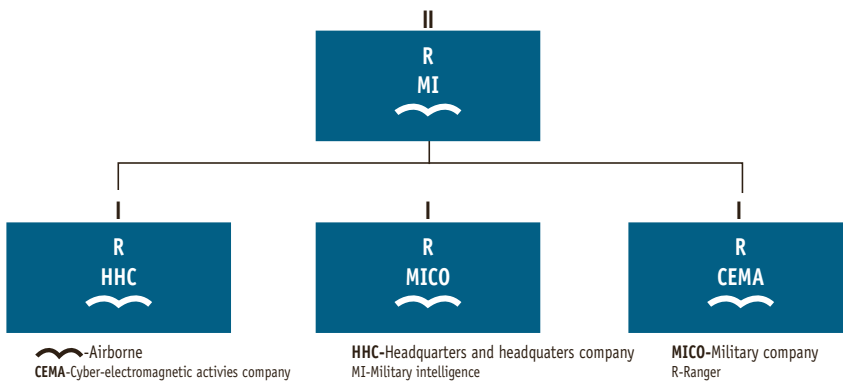


Figura 3: Orgánica del Batallón de Inteligencia de Rangers, donde se destaca una UF con capacidad CEMA.

Fuente: The 75th Ranger Regiment Military Intelligence Battalion Modernizing for Multi-Domain Battle.

BRIGADAS DIGITALES[27] DE LA FUERZA TERRESTRE

Las BRIACOs con que actualmente cuenta la Fuerza Terrestre son UACs altamente tecnologizadas, que emplean ampliamente el ciberespacio y el espectro electromagnético como medios de transmisión y recepción de voz, datos e imagen con grandes anchos de banda y altas velocidades de transmisión para que los diferentes comandantes puedan conducir las operaciones de alta intensidad y con un *tempo*[28] superior al adversario.

---

25 Brigade Combat Team.

26 Deliberada emisión de energía electromagnética sobre un receptor con el propósito de reducir el uso del espectro electromagnético por parte del enemigo, además de neutralizar y degradar su capacidad de mando y control. (ATP-336 Electronic Warfare Techniques).

27 La primera brigada digital fue creada en el Ejército de EUA en el año 1996, dentro del programa *Force XXI Battle Command Brigade and Below*. Dicha UAC se caracterizaba por contar con sistemas de comunicaciones digitales, con capacidad de transmitir voz, datos e imagen con gran ancho de banda, lo cual permitía a los comandantes tener "conciencia situacional" en tiempo real respecto a fuerzas propias, fuerzas adversarias, terreno y tiempo atmosférico. Department of the Army, Field Manual, *Armored and Mechanized Brigade Operations*-FM 71-3, 08 January, 1996.

28 El *tempo* es un concepto que se refiere a la velocidad en la toma de decisiones, velocidad en la ejecución de las órdenes y velocidad en la transición entre una actividad y la próxima.

A modo de ejemplo, una BRIACO, dependiendo de la respectiva ORGATAR, despliega más de 90 redes de comunicaciones[29] de voz, datos y redes mixtas para integrar las diferentes funciones de combate dentro del sistema operativo, empleando además los siguientes medios tecnológicos:

- SICOE (Sistema de Comunicaciones del Ejército) Microondas.
- Enlaces HCLOS (High Capacity Line of Sight) Microondas.
- Plataformas satelitales VSAT (Ku), INMARSAT, BGAN.[30]
- Fibra óptica y cableado estructurado (UTP, FTP).
- Sistemas de comunicaciones HF/VHF/UHF HARRIS, ELBIT, TADIRAN, MARCONI, JAGUAR.
- Computadores Toughbook Panasonic rugedizados.
- Panoramas tácticos TORCH y BMS[31] (C2).
- GPS Banda Ku asociados a sistemas C2.
- Protocolo HQ II. (Enlace encriptado aire-aire y aire-tierra).
- Radares THALES Banda Ku y ELTA Banda L.
- Sistema de control de fuego AFATDS (Advanced Field Artillery Tactical Data System).
- Plataformas UAVs SKYLARK y Drones PHANTOM.[32]

En síntesis, las BRIACOs dependen de las TICs, así como del espectro electromagnético y del ciberespacio para que la plataforma tecnológica y el sistema C4ISR pueda ser eficiente en la conducción de operaciones. Asimismo, es altamente vulnerable a la acción de la guerra electrónica y de las ciberoperaciones del adversario. Conforme a lo expuesto, resulta esencial la protección de los nodos críticos de mando y control, así como de todos los activos de información que se encuentran almacenados en los terminales tácticos y discos duros que forman parte de los anillos de comunicaciones de los diferentes puestos de mando, además de la protección de las comunicaciones radiales de voz, datos e imagen que emplean enlaces HF/VHF/UHF para la transmisión de órdenes gráficas, FRAGOS, OPORDs, así como información operativa y de carácter logístico entre los diferentes escalones, lo cual, de ser detectado o degradado por el adversario, causaría un gravísimo daño a la seguridad militar y a la conducción de las operaciones por parte de los comandantes de todos los niveles.

---

29 Una BRIACO despliega cerca de 90 redes de voz, datos y mixtas desde el nivel de comando de brigada hasta el nivel de sección y pelotón, pasando por establecer redes de mando, redes ISR, redes logístico-administrativas, red escalón superior, enlaces tierra-aire para EVACAM y apoyo aéreo estrecho con protocolos Have Quick II. (Datos entregados por la Compañía de Telecomunicaciones de la BRIACO "Coraceros", conforme a la experiencia en maniobras y ejercicios).

30 VSAT (Very Small Aperture Terminal), antena satelital fija que usa la banda "X" con una banda de subida de 7,9 a 8,4 Ghz y una frecuencia de bajada entre los 7,25 y 7,75 Ghz. Los medios BGAN tienen la capacidad de transmitir voz y datos a 492 kbps.

31 *Battle Management System*. Sistema de C2 que permite transmisión y recepción de voz, datos, calcos y órdenes gráficas mediante equipos de radio con integración en banda ancha con dispositivos computacionales.

32 La mayoría de los drones en el mercado emplean el ciberespacio a través de Internet para geolocalizar el aparato y para transmitir y recibir información. Por otro lado, usan señales de recepción GPS para navegar y el espectro electromagnético a través de enlaces de radio para comunicarse con el operador.

Figura N° 4: Relación de CEMA con medios, TICs y sistemas que usan el espectro electromagnético y el ciberespacio para su operación.

Fuente: Elaboración del propia.

LAS FUERZAS DE TAREAS Y EQUIPOS CEMA: UNA CAPACIDAD MILITAR POLIVALENTE

Este nuevo concepto de capacidad militar obedece a la necesidad de contar con unidades especialistas en inteligencia, guerra electrónica y ciber-operaciones, con una alta disponibilidad, despliegue rápido, modular y altamente polivalentes con el propósito de realizar tareas de carácter defensivo y ofensivo tanto en el espectro electromagnético así como en el ciberespacio, además de constituir una unidad altamente especializada como medio de obtención y con la capacidad de integrarse a un elemento de apoyo ISTAR, como parte de un CCMO[33] o una CPDI,[34] en apoyo al sistema o arquitectura de inteligencia de una UAC de magnitud de brigada o división en tiempo de crisis, EPB y también en tareas enmarcadas en el contexto de MOOTW. Dentro de las capacidades con que cuentan estas unidades, se destacan las siguientes:

- Inteligencia de Comunicaciones (COMINT).
- Control de Emisiones (EMCON).
- Radiolocalización de emisiones de interés.(Direction Finding[35]).
- Tareas de obtención en fuentes abiertas (OSINT).
- Ciber ISR.
- Seguridad informática sobre nodos y anillos de comunicaciones.

33 Centro Coordinador de Medios de Obtención.
34 Centro de Producción y Difusión de Inteligencia.
35 Acción de guerra electrónica que permite realizar búsqueda, interceptación y localización de emisiones de interés, con el propósito de determinar a ubicación exacta en el terreno de nodos de comunicaciones, puestos de mando y centrales de radio adversarios.

- Ciberoperaciones defensivas (DCO).
- Ciberoperaciones ofensivas (OCO).[36]

EQUIPOS CEMA

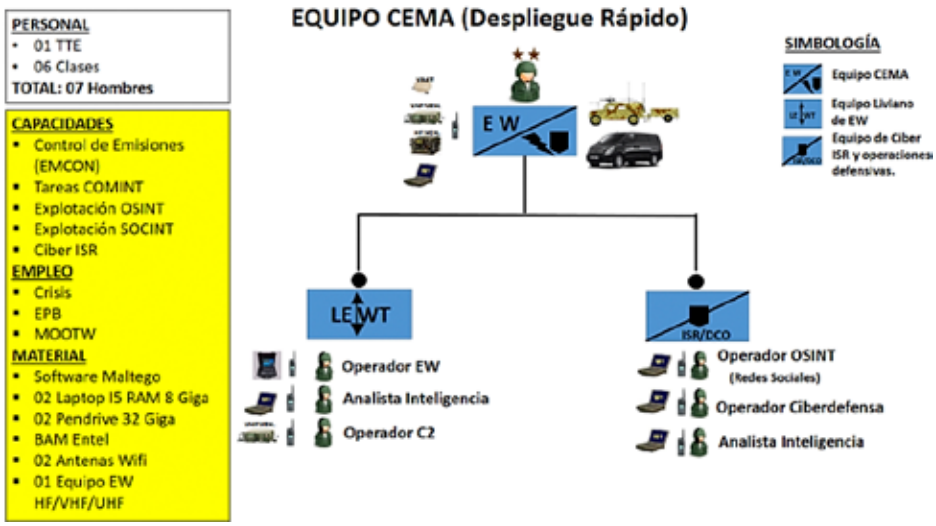


Figura N° 5: Equipo CEMA compuesto a base de especialistas en inteligencia y guerra electrónica.

Fuente: Elaboración del propia.[37]

Los equipos CEMA son unidades livianas, modulares y de despliegue rápido con una autonomía logística de 72 horas, con la capacidad de integrarse a una FT CEMA o FTs de Inteligencia dependiendo de la misión, escenario y tareas asignadas, e integrando capacidades de obtención en el ciberespacio y en el espectro electromagnético como parte del sistema de inteligencia o elemento de apoyo ISTAR de una UAC de magnitud de brigada o división. Constituyen una capacidad militar por cuanto poseen medios de mando y control C2 a base de material HF/VHF/UHF de voz y datos protegidos, sistemas EW y ciberportátiles, autonomía logística relativa en cuanto a mantenimiento y abastecimiento, así como infraestructura, personal entrenado y medios radicados en las unidades de Inteligencia en tiempo de paz, conforme a la doctrina de inteligencia, guerra electrónica y ciberoperaciones. Son una capacidad polivalente por cuanto pueden actuar en crisis, EPB y MOOTW en forma rápida y coordinada, y no solamente en misiones de obtención, sino también en tareas defensivas y ofensivas en el ciberespacio y espectro electromagnético, conforme a la situación y necesidad del escalón superior.

36 Vectores de ataque tales como malware, spyware, ataques DoS, ataques de día cero, ransomware, ingeniería social, gusanos de red, troyanos, phishing, entre otras acciones ofensivas.

37 Elaboración propia basada en la norma militar MIL-STD-2525D, *Joint Military Symbology*. Al respecto, cabe señalar que la doctrina nacional aún no considera simbología militar para las ciberoperaciones.

FUERZA DE TAREAS CEMA

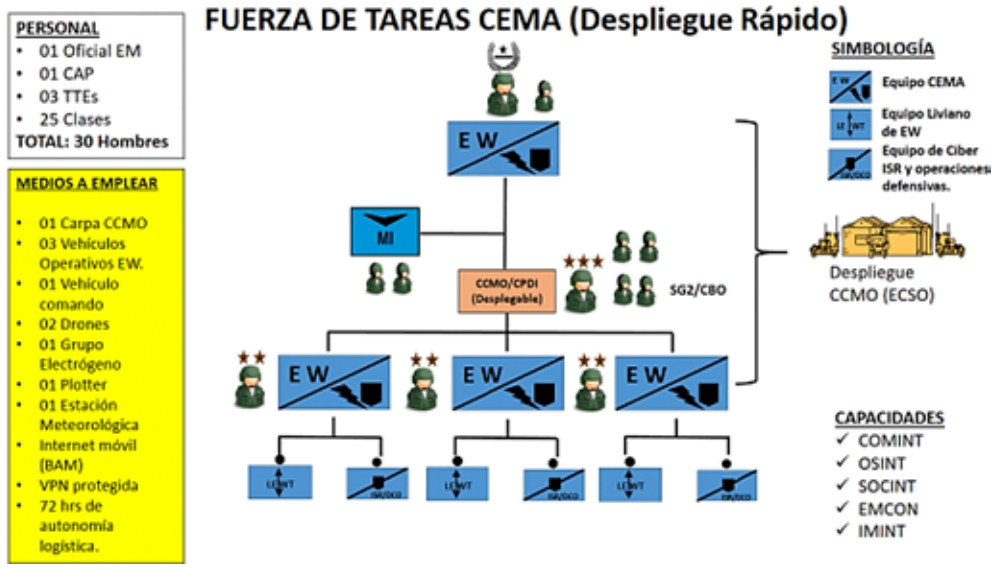


Figura N° 6: Fuerza de Tareas CEMA organizada a base de integración de capacidades COMINT, OSINT, IMINT y CIBERISR.

Fuente: Elaboración del propia.

La FT CEMA es una unidad militar de Inteligencia conformada bajo el concepto de ORGATAR y con la capacidad de integrar capacidades militares de obtención en el ciberespacio y en el espectro electromagnético, organizando bajo un mando único con medios de EW COMINT, CIBERISR, OSINT e IMINT a base de una unidad de drones. En el caso de la imagen, la FT CEMA cuenta con tres equipos CEMA y una unidad de drones, coordinados e integrados mediante un CCMO como organismo dependiente de un elemento de apoyo ISTAR a nivel de una UAC o cuartel general desplegado.

Esta unidad puede concurrir con su personal y medios técnicos en apoyo UACs de magnitud de división o brigada, así como en beneficio de tareas de obtención del OMOE[38] e incluso a nivel conjunto integrados a un CENFIC[39] y a una EWCC[40] pertenecientes a la arquitectura de inteligencia de un TOC.

UNIDAD ANTIDRONES: CAPACIDAD MILITAR EMERGENTE Y NECESARIA

Los drones militares y civiles de bajo costo se han transformado en los últimos años en una amenaza real por parte de fuerzas convencionales y no convencionales, los cuales pueden ser

38 Órgano de Maniobra de Operaciones Especiales.
39 Centro de Fusión de Inteligencia Conjunto
40 Célula de Coordinación de Guerra Electrónica.

empleados como eficientes plataformas de ISR con empleo diurno y nocturno, así como vectores de ataque contra infraestructura crítica y objetivos de alto valor (HVTs). Como ejemplo de la preocupación que existe a nivel mundial por esta nueva amenaza, el Ejército de EUA ha incrementado fuertemente la inversión en tecnologías y medios antidrones, firmando un contrato con la empresa Leonardo por un total de $42 millones de dólares para desarrollar un sistema antidrone llamado Mobile Low, Slow Unmanned Aerial Vehicle Integrated Defense System[41] (MLIDS), combinando sensores, radares y armas o jammers electromagnéticos para degradar drones militares y civiles de bajo costo, los cuales están siendo empleados con éxito por las fuerzas de ISIS y fuerzas rebeldes en el conflicto de Siria en contra de fuerzas estadounidenses y rusas. A nivel sudamericano, el Ejército de Brasil empleó con éxito unidades antidrones equipadas con jammers de fabricación propia durante la Copa del Mundo y los Juegos Olímpicos.[42]

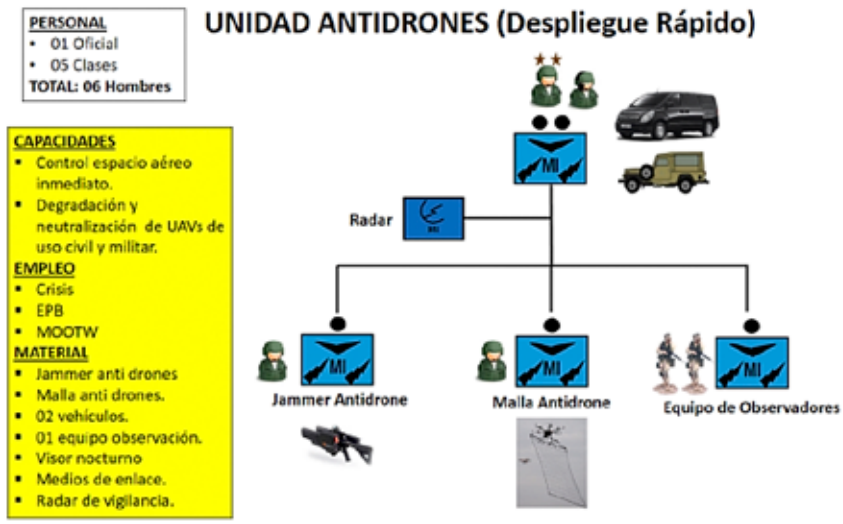


Figura N° 7: Sección Antidrones equipada con radar de vigilancia, equipos de observación, jammer y mallas.

Fuente: Elaboración del propia.

La unidad propuesta estaría equipada con un jammer antidron cuya función es neutralizar y degradar las señales GPS y electromagnéticas del dron, evitando que reciba y transmita datos e imágenes. Asimismo, contaría con un radar de vigilancia con la capacidad de entregar alerta temprana, trayectoria y ubicación del dron durante su aproximación. Por otro lado, se desplegaría un equipo de observación con el propósito de complementar el trabajo de alerta temprana del radar y finalmente se emplearía un dron propio equipado con malla con el propósito de capturar o derribar el dron hostil. Esta unidad podría integrarse a una FT CEMA o una FT de Inteligencia en

41 CEBUL, Daniel (2018). "US Army increases investment on counter-drone program", C4ISR.NET.

42 La unidad Antidrones del Ejército Brasileño se encuentra encuadrada en el Batallón de Guerra Electrónica con asiento en Brasilia. (Antecedentes obtenidos por el autor durante la visita a dicha unidad en agosto de 2017).

apoyo de unidades de la Fuerza Terrestre conforme a requerimiento y durante eventos masivos en apoyo de unidades de seguridad militar.

CONCLUSIONES

El dominio y la libertad de acción en el espectro electromagnético y en el ciberespacio resulta esencial para que la Fuerza Terrestre pueda mantener la iniciativa, superioridad de información, así como un tempo y ciclo OODA superior al adversario.

Las brigadas digitales y casi la totalidad de los sistemas de armas y medios de mando y control de la Fuerza Terrestre emplean el ciberespacio y espectro electromagnético como medios para apoyar y conducir las operaciones, por lo cual la superioridad en dichas dimensiones resulta esencial y crítico.

La experiencia y lecciones aprendidas de la OTAN, así como del Ejército de Rusia, permiten concluir que la guerra electrónica y las ciberoperaciones son una eficiente herramienta de obtención de información cuya fusión bajo el concepto de CEMA permitiría mayor eficiencia y sinergia en el empleo de medios humanos y materiales en tareas ISR, así como en operaciones defensivas y ofensivas en el ciberespacio y en el espectro electromagnético.

Las unidades CEMA (FT y equipos) y unidad antidrones representan una capacidad militar de alta disponibilidad y especialización técnica que permite administrar y explotar el ciberespacio y el espectro electromagnético en beneficio de la Fuerza Terrestre, además de negar su uso a la amenaza, constituyendo un nuevo multiplicador de combate.

BIBLIOGRAFÍA

ADRP 6-0 "Mission Command", Headquarters Department of the Army, May 2016.

ALANIZ, Osvaldo (2018). *Las actividades ciber-electromagnéticas: un combate invisible*, CESIM.

APPLEGATE, Scott (2012). *The Principles of Maneuver in Cyber Operations,* George Mason University, Fairfax Virginia, .

CEBUL, Daniel (2018). *US Army increases investment on counter-drone program,* C4ISR.NET

DELACRUZ, Víctor (2016). "Mission Command in and Through Cyberspace: A Primer for Army Commanders", *The Army Press,* Fort Levenworth Texas.

Ejército de Chile, DIVDOC, DD-10001, "El Ejército y la Fuerza Terrestre", 2010.

Ejército de Chile, DIVDOC, RDI-20008, Reglamento Ciberdefensa, 2016.

Ejército de Chile, DIVDOC, RAA-03008 "Proceso de Desarrollo de Capacidades Militares", Edición 2013

EOM, Jung Ho, "Roles and Responsabilities of CyberIntelligence for Cyber Operations in Cyberspace", *Military Studies,* Daejeon University, 2014.

FM 3-12 "Cyberspace and Electronic Warfare Operations", Headquarters Department of the Army, April 2017.

FM 3-36, "ElectronicWarfare", Headquarters Department of the Army, November 2012.

FM 3-38 "Cyber Electromagnetic Activities", Headquarters Department of the Army, February 2014.

FOXALL, P, "Putin´s Cyberwar: Rusia´s Statecraft in the Fifth Domain", Russia Studies Centre, Policy Paper N°16, May 2016.

JOINT Publication, 3-12, "Cyberspace Operations", February 2013.

LAMOTHE, Dan (2017). "How the Pentagom´s Cyber Offensive against ISIS could shape the future for elite US forces". *The Washington Post*

McCROSKEY, Erick (2017). *Operational Graphics for Cyberspace,* JFQ.

MADOC, DO2-007, "Doctrina de Guerra Electrónica", Ejército de Tierra de España, 2001.

MoD, Joint Doctrine Note 1/18 "Cyber and Electromagnetic Activities", Chief of Staff, febrero de 2018

POMERLAU, Marc. *How the Army will infuse cyber operations on the battlefield.*

PORCHE, Isaac; PAUL, Christopher; SERENA, Chad; CLARKE, Colin; JOHNSON, Erin; HERRICK, Drew (2017). *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below,* RAND Corporatio.

QUINTANA, Yolanda (2016). *Ciberguerra*, Editorial Catarata, Madrid.

SCHACHTMAN, N. (2009). *Insurgents intercepts Drone Video In King-Size Security Breach*.

UNDERWOOD, Kimberly (2018). *Army CEMA Teams Advance Information, Electronic and Cyber Warfare,* August 6.

METODOLOGÍA PARA EL DISEÑO DE ARQUITECTURAS DE SISTEMAS DE MANDO Y CONTROL PARA LA GESTIÓN DEL RIESGO DE DESASTRES (GRD)[1]

TENIENTE CORONEL JOSÉ LLANOS ACEVEDO[2]

RESUMEN: *el Marco de Sendai para la reducción del Riesgo de Desastres 2015-2030[3] declara en su Prioridad 4 que todos los países deben desarrollar mecanismos de comunicación de emergencias y riesgo de desastres. Por otra parte, en lo referido a situaciones de emergencia, desastre o catástrofe, Chile ocupa el 1er lugar de pérdidas económicas por desastres, dentro de otros países del G20 con similar porcentaje de PIB.[4] A este respecto, el presente paper pretende, en forma muy resumida y conceptual, entregar una metodología basada en Ingeniería de Sistemas y Arquitecturas, con la finalidad de diseñar sistemas de mando y control para la gestión del riesgo de desastres.*

Palabras clave: *gestión del riesgo de desastres, mando y control, toma de decisiones, ingeniería de sistemas, conciencia situacional.*

Abstract: *in its Priority 4, the Sendai Framework for Disaster Risk Reduction 2015-2030 states, that all countries should develop mechanisms for communication of emergencies and risks of disasters. On the other hand, in the context of emergency, disaster or catastrophe situations, Chile ranks 1st. in economic loss due to disasters among other G20 countries with similar percentage of GDP.Therefore, the present paper intends, in a very brief and conceptual way, to deliver a methodology, based on Systems Engineering and Architectures, in order to design command and control systems for Risk and Disaster Management.*

---

1 Artículo ganador del tercer puesto del concurso "Desarrollando Capacidades Militares", en el ámbito de Ciencias Militares, Combate, Generación de Doctrina y Docencia.

2 Oficial de Ejército, Ingeniero Politécnico Militar mención Comunicaciones, magíster en Ciencias de la Ingeniería mención Mando y Control y magíster en Planificación y Gestión de Riesgos de Desastres.

3 United Nations (en línea). Marco Sendai para la Reducción del Riesgo de Desastres (2015-2030), disponible a través de: https://www.unisdr.org/files/43291_ spanishsendaiframework fordisasterri.pdf

4 Consejo Nacional de Innovación para el Desarrollo Hacia un Chile Resiliente frente a Desastres: una oportunidad (en línea). Santiago de Chile, 2016 p. 14. Disponible a través de http://www.cnid.cl/wp-content/uploads/2016/12/CREDEN-27122016-2.pdf

Keywords: *disaster risk management, command & control, decision making, systems engineering, situation awarness.*

INTRODUCCIÓN

Al igual que la guerra, los desastres son poco estructurados en cuanto al flujo de información, ya que para su manejo están involucrados varios entes, los cuales usan distintos medios para transmitir y recibir información. Además de reinar la incertidumbre y el caos, el tiempo se hace cada vez más escaso, sobre todo dentro de los primeros minutos de sucedido los desastres.

Es así que, según Esteve, *"en este tipo de operaciones, desde el punto de vista del mando y control, es fundamental adquirir una visión global de la situación mediante el intercambio de cada unidad de percepción de la situación".*[5]

Por otra parte, Jobidon, Labrecque, Turcotte, Rousseau & Tremblay afirman que *"las situaciones son más complejas y dinámicas, [por lo que] requieren que los individuos tomen decisiones óptimas bajo restricciones de alto riesgo, incertidumbre, alta carga de trabajo y presión de tiempo".*[6]

A su vez, según Meissner, Luckenbach, Risse, Kirste & Kirchner,[7] es de alta importancia la coordinación e integración de la información en estos momentos, *"dado que la coordinación requiere información actual, y debe ser comunicada en sentido ascendente y descendente dentro y entre las organizaciones en tiempo real, [por lo cual] surge la necesidad de un sistema integrado de comunicación e información para la gestión de desastres".*

Finalmente, según Ogasawara, Tanimoto, Imaichi y Yoshimoto, *"durante un desastre, las actividades de respuesta deben operar en un entorno en constante cambio. Por esta razón, las soluciones de apoyo a la prevención y respuesta a las catástrofes se basan en el concepto de implementar el ciclo de observar, orientarse, decidir y accionar",*[8] comúnmente llamado ciclo de Boyd.

---

5 ESTEVE, Manuel, C4ISR Multimedia System for Emergency Management TIN2004-03588, (en línea). Trad. del autor. Valencia, Departamento de Comunicaciones Universidad Politécnica de Valencia. (2016). p.4.

6 JOBIDON, Marie Eve; LABRECQUE, Alexandre; TURCOTTE, Isabelle; ROUSSEAU, Vincent y TREMBLAY, Sébastien (2007). Adaptability in Crisis Management: The Role of Organizational Structure (en línea). Trad. del autor. Toronto: Defence R&D Canadá-Toronto, p.3.

7 MEISSNER, Andreas; LUCKENBACH, Thomas; RISSE, Thomas; KIRSTE, Thomas y KIRCHNER, Holger (2002). Design Challenges for an Integrated Disaster Management Communication and Information System, (en línea). Trad. del autor. Berlín: Institute for Open Communication Systems, p. 1.

8 OGASAWARA, Junji; TANIMOTO, Koichi; IMAICHI, Osamu y YOSHIMOTO, Masayoshi (2014). Disaster Prevention and Response Support Solutions, (en línea). Trad. del autor. Hitachi Review, p. 2.

EL CICLO BOYD

El ciclo Boyd, también conocido como ciclo de la decisión, ciclo OODA o ciclo de mando y control, se encuentra ligado directamente a la conciencia situacional *(situational awareness)*,[9] donde el coronel Boyd[10] vio al enemigo como un sistema que actúa a través de un proceso de toma de decisiones basado en las observaciones del mundo que lo rodea. Según Brehmer, la visión de Boyd *"les permitió entrar en el ciclo de decisiones del enemigo y ganar el combate".*[11]

Por otra parte, este ciclo ha estado en permanente análisis ante eventos de gran magnitud que afecten a la población y se han perseguido esfuerzos por adaptarse a él.

De acuerdo con Chumer y Turoff,[12] el *"punto de partida para la teoría de mando y control en este tipo de eventos son los cuatro pasos o elementos de proceso del ciclo Boyd",*[13] los que corresponden observar.

Esto es, la percepción de los objetos que nos rodean normalmente, lo que si bien ocurre de forma visual, es un proceso en el que todos los sentidos están involucrados con la tecnología existente; el orientarse, que se refiere a que tanto la orientación cognitiva individual como la colectiva sobre los datos que se perciben y se comunican están asociadas a las tecnologías de visualización, por lo que ayudan a la función de mando y control; el decidir, que tiene relación con que el ser humano siempre está esforzándose o luchando para obtener un sentido de lo que es la realidad para poder tomar la decisión más acertada en las circunstancias de estos eventos; y, finalmente, el accionar, que corresponde a la capacidad de comunicar la acción sugerida y, luego, controlar la acción con el fin de determinar si la planificación y acciones que se han decidido se dan de la mano con las expectativas establecidas en el marco de las decisiones de las autoridades, es decir, la intención de ambas partes en las distintas operaciones.

---

9 ALBERTS, David; GARSTKA, John, y STEIN, Frederick. Network centric warfare: developing and leveraging information superiority. United state of America: CCRP Commnad and control research program. 1999, p. 140. Trad. del autor. *La conciencia situacional, o *situational awareness*, es la percepción de un individuo de la información sobre la situación y existe en todo o en parte del espacio de batalla en un momento determinado y se trata de lo que las personas saben de la situación actual y emergente.

10 OSINGA, Frans. Science, Strategy and War the Strategic Theory of John Boyd. p.2. Amsterdam: Eburon Academic Publishers, (en línea). Trad. del autor. 2005, p. 2. *El coronel John Boyd era un oficial en la Fuerza Aérea de Estados Unidos que vivió entre 1927 y 1997, es el creador del ciclo de Boyd o OODA.

11 BREHMER, Berndt. The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control. Stockholm: Department of War Studies Swedish National Defence College, 2006, p.3. Trad. del autor.

12 CHUMER, Michael y TUROFF, Murray. Command and control (C2): Adapting the distributed military model for emergency response and emergency management, (en línea). New Jersey: New Jersey Institute of technology, 2005, p. 2. Trad. del autor.

13 BREHMER, Berndt. *Op cit.*, p. 3. *El ciclo OODA de Boyd (observar-orientar-decidir-actuar) es claramente el modelo dominante de mando y control hoy en día.

CICLO DE LA GESTIÓN DEL RIESGO DE DESASTRES (GRD)

La gran mayoría de los estamentos que participan en la gestión de un desastre centra la totalidad de sus esfuerzos desde que ocurre el evento hasta la respuesta, sin saber que existen otras fases donde pueden operar de forma más eficiente y eficaz, a través de actividades de las fases previas.

Como afirma Tood y Tood,[14] las fases del ciclo de GRD son: predesastre, respuesta, postdesastre, como lo indica la figura N°1.

Por otra parte, el Plan Estratégico Nacional para la Gestión del Riesgo de Desastres (PENGRD) define las fases prevención, mitigación, preparación, respuesta y rehabilitación, y recuperación como ámbitos de acción[15] de la GRD. Es por esto que la respuesta se puede relacionar directamente con el ciclo Boyd (OODA), debido a que se debe actuar inmediatamente después de ocurrido el desastre con el propósito de acelerar el ciclo de toma de decisiones de las autoridades.

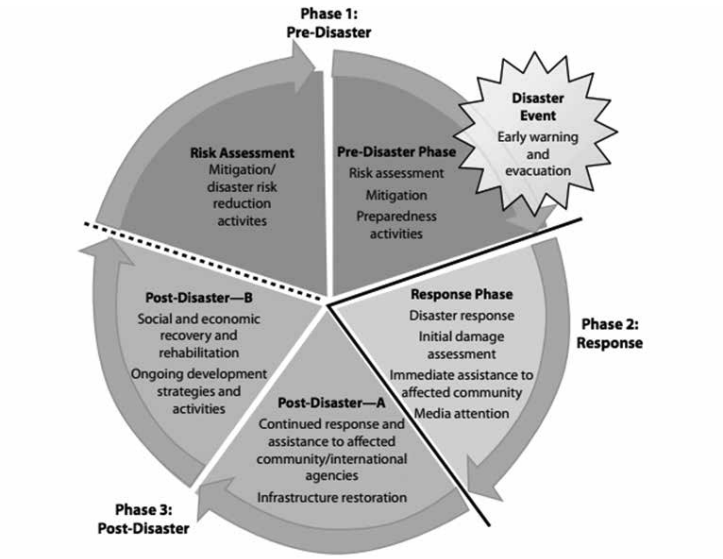


Figura N° 1: "Fases del ciclo de gestión del riesgo de desastres".

Fuente: TODD, David; TODD, Hazel. Natural Disaster Response: Lessons from Evaluations of the World Bank and Others (en línea). Evaluation Brief; 16. Washington, DC.: World Bank. 2011, p. 4.

Disponible en: https://openknowledge.worldbank.org/handle/10986/27353 License: CC BY 3.0 IGO.

14 TOOD, David; TOOD, Hazel. Natural disaster response, independent evaluation group, (en línea). Washington, DC.: World Bank, 2011, p. 3. Trad. del autor. *Se entiende que estas fases no tienen límites claros, sino que se superponen cronológicamente, así como en términos de las actividades en curso. Washington: Independent Evaluation Group Communications, Learning, and Strategy.

15 Ministerio del Interior y Seguridad Pública. Plan Estratégico Nacional para la Gestión del Riesgo de Desastres, Santiago: ONEMI, 2015, p. 31.

Es así que se hace necesario una plataforma tecnológica que permita lo anterior, tal como postula Ogasawara, Tanimoto, Imaichi & Yoshimoto, porque esta ayuda *"a trabajar a través del ciclo OODA de forma rápida y precisa durante un desastre de gran tamaño, tales como monitorización y detección de anomalías, análisis de la situación y solución de predicción, mando y control para el socorro y la recuperación, solución de apoyo al trabajo en casos de desastre"*.[16]

La guerra y los desastres se caracterizan porque nadie puede predecir la hora de los eventos de gran magnitud. De esta manera, la GRD toma un papel fundamental y el rol que juegan las autoridades, junto con el manejo de la información, es clave. De ahí nace la enorme necesidad de contar con un sistema de mando y control (SMC) para manejar de mejor manera la incertidumbre, la variabilidad y la complejidad de la situación.

Como afirma Arroyo de la Rosa, las características del enlace en emergencias *"obedecen a los conceptos de tecnologías de la información en emergencias, las que condicionan la tarea como: redes no disponibles, sistemas no fiables, problemas de interoperabilidad, diversidad de usuarios, urgencia de la información tramitada, insuficiencia de medios, indisciplina e intrusismo en las redes"*.[17] Por otra parte, Esteve observa que se da la misma dinámica en el mundo militar, ya que *"el objetivo de los sistemas militares de información de mando y control es elaborar el panorama operacional común (POC) y que es tremendamente necesario usar esta funcionalidad a la gestión civil de emergencias"*.[18] A su vez, Ogasawara, Tanimoto, Imaichi y Yoshimoto aseguran que es necesario un *"sistema rápido de evaluación de la situación que utiliza información y otras fuentes inmediatamente después del desastre para ayudar a recopilar información rápidamente y determinar lo que está sucediendo para asegurar la toma de decisiones en tiempo real"*.[19]

Si bien es cierto que todas las fases del ciclo gestión del riesgo de desastres son importantes, la necesidad real de acelerar el ciclo de toma de decisiones se hace fundamental en la fase de respuesta, debido al gran flujo de información y la necesidad de que las autoridades tomen las decisiones más acertadas posibles.

---

16 OGASAWARA, *et al. op. cit.,* p. 29.

17 ARROYO de la Rosa, Rodolfo. "Las transmisiones militares en emergencias: un terreno nada desconocido". *Revista Ejército de Tierra de España,* 2014, p.31.

18 ESTEVE, Manuel. *Op. cit.,* p. 4

19 OGASAWARA, *et al. op. cit.,* p. 33.

METODOLOGÍA PARA EL DISEÑO DE UNA ARQUITECTURA DE SISTEMA DE MANDO Y CONTROL PARA LA GRD

Introducción a la metodología

En el panorama actual, el crecimiento de los sistemas complejos que interactúan con otros sistemas en forma dinámica hace que estos[20] se comporten de manera inesperada.

Por lo anterior, contar con un pensamiento sistémico[21] es clave para entender el comportamiento dinámico dentro de los sistemas. Senge, líder en esta materia a nivel mundial, define el pensamiento sistémico *"como una disciplina para ver el todo y un marco para ver las interrelaciones en lugar de las cosas, para ver los patrones de cambio en lugar de estática instantáneas".*[22]

La tecnología trae asociado que un sistema diseñado es parte de otro sistema.

En otras palabras, nos encontramos frente a sistemas de sistemas[23] que pueden ser conducidos directamente al fracaso si es que no es bien manejada la complejidad.

Todos estos sistemas se alimentan entre sí para producir efectos extremadamente complejos e impredecibles.

La norma ISO/IEC 15288 define este concepto *"como una colección interoperable de sistemas componentes que producen resultados inalcanzables".*[24]

Pasos del proceso de diseño de sistemas

El presente *paper* se centra en la metodología para el diseño de un sistema a través de la ingeniería de sistemas, por lo que es necesario conocer este concepto.

---

20 Department of Defense United State of America. Systems Engineering Fundamentals, (en línea), Virginia: Supplementary text prepared by the defense acquisition University Press Fort Belvoir, 2001, p.3. Trad. del autor. *Un sistema es un compuesto integrado de personas, productos y procesos que proporcionan una capacidad para satisfacer una necesidad u objetivo declarado.

21 ARNOLD, Ross y WADE, Jon. A Definition of Systems Thinking: A Systems Approach, (en línea). Nueva York: Elsevier B.V., 2015, p. 7. Trad. del autor. *El pensamiento sistémico es un conjunto de habilidades analíticas sinérgicas utilizadas para mejorar la capacidad de identificar y la comprensión de los sistemas, predecir sus comportamientos e idear modificaciones en ellos para producir los efectos deseados.

22 SENGE, Peter (1990). *The Fifth Discipline, The Art and Practice of the Learning Organization.* Trad. del autor. New York: Doubleday/ Currency.

23 Department of Defense United State of America. Systems Engineering Guide for Systems of Systems, (en línea), 2008, p. 4. Trad. del autor. *Sistemas de sistemas se define como un conjunto o arreglo de sistemas que resulta cuando sistemas independientes y útiles se integran en un sistema más grande que proporciona capacidades únicas.

24 La norma ISO / IEC 15288 establece un marco común para describir el ciclo de vida de los sistemas creados por los seres humanos y define un conjunto de procesos y la terminología asociada dentro de ese marco.

En primer lugar, el International Council on Systems Engineering (INCOSE) lo define como *"un enfoque interdisciplinario y medios para permitir la realización de sistemas exitosos".*[25]

Por su parte, la National Aeronautics and Space Administration (NASA) lo define como *"una disciplina holística e integrativa, en la que se evalúan y equilibran las contribuciones de los ingenieros estructurales, ingenieros eléctricos, diseñadores de mecanismos, ingenieros de potencia, ingenieros de factores humanos y muchas otras disciplinas, para producir una coherencia de todo lo que no está dominado por la perspectiva de una sola disciplina".*[26]

Para el Mil-Std 499A, este concepto corresponde a *"una secuencia lógica de actividades y transformación de la necesidad operativa en una descripción del sistema, los parámetros de rendimiento y una configuración de sistema".*[27]

Finalmente, Buede afirma *"que es una disciplina que se centra en el diseño y aplicación de todo (sistema) como distinto de las partes. Implica mirar un problema en su totalidad, teniendo en cuenta todas las facetas y todas las variables y relacionando lo social con lo técnico".*[28]

Por otro lado, el proceso de actividades de ingeniería de sistemas que declara el Departamento de Defensa de Estados Unidos está compuesto por el análisis de requisitos, el análisis funcional y la síntesis de diseño.

INCOSE define el análisis de requisitos como "*revisar, evaluar, priorizar y equilibrar todos los requerimientos de las partes interesadas y transformar esos requisitos en una visión funcional y técnica de una descripción del sistema capaz de satisfacer las necesidades de las partes interesadas".*[29]

NASA, por su parte, define este concepto como *"transformar las expectativas de las partes interesadas en una definición del problema y luego en un conjunto completo de requisitos expresados como declaraciones de uso que pueden emplearse para definir una solución de diseño".*[30]

---

25 International Council on Systems Engineering, INCOSE (2003). *Systems Engineering Handbook a Guide for System Life Cycle Processes and Activities.* San Diego: Cecilia Haskins, p. 20. Trad. del autor.

26 National Aeronautics and Space Administration, NASA. Systems Engineering Handbook (en línea), Washington: NASA Headquarters, 2007, p. 3. Trad. del autor.

27 Department of Defense United State of America (1974). *Military Engineering Standard Management.* Washington: Air Force Sytems Command, p. 3. Trad. del autor.

28 BUEDE, Dennis (2009). *The Engineering Design of System, Models and Methods,* New Jersey: A John Wiley & Sons, p. 5. Trad. del autor.

29 INCOSE (2003). *Systems Engineering Handbook a Guide for System Life Cycle Processes and Activities.* San Diego: Cecilia Haskins, p. 52.

30 NASA (2007). *Systems Engineering Handbook.* Washington: NASA Headquarters, p. 40. Trad. del autor.

Buede, en tanto, define que, en esta parte del proceso, *"los ingenieros de sistemas toman estos requisitos de nivel alto de las partes interesadas y derivan un conjunto consistente de declaraciones de ingeniería más detalladas de los requisitos a medida que avanza el diseño".*[31]

Por su parte, MITRE establece que *"después de evaluar las necesidades operacionales, lo siguiente es descubrir, obtener, recopilar, definir y analizar los requisitos donde se analizarán, transformarán e integrarán las necesidades de los usuarios en los requisitos del sistema".*[32]

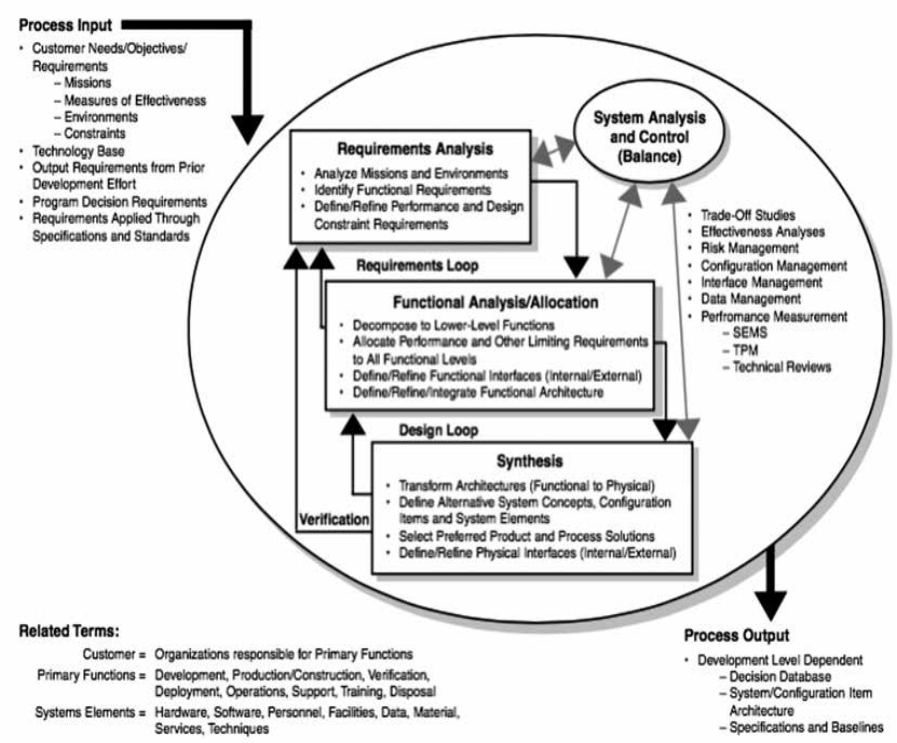


Figura N° 2: "Proceso de Ingeniería de Sistemas".

Fuente: Department of Defense United State of America Systems Engineering Fundamentals, Virginia: Supplementary text prepared by the Defense Acquisition University press Fort Belvoir, 2001, p.6.

Posteriormente, cobra vital importancia realizar el análisis funcional. Blanchard lo define como *"el proceso iterativo de estructurar o descomponer los requisitos del nivel sistema, a los subsistemas, y tan abajo en la estructura jerárquica como sea necesario para identificar los recursos específicos y los distintos componentes del sistema".*[33]

31 BUEDE, Dennis. *Op. cit.*, p. 30

32 MITRE (2014). *Systems Engineering Guide.* p. 305. The MITRE Corporate Communications and Public Affairs, p. 305. Trad. del autor.

33 BLANCHARD, Benjamín (1995). *Ingeniería de Sistemas.* Madrid: Isdefe, p.19.

Por otro lado, el Departamento de Defensa de Estados Unidos afirma que este proceso es para *"especificar sucesivamente requisitos de funcionalidad y desempeño de nivel inferior, definiendo así arquitecturas con niveles cada vez mayores de detalle. Los requisitos del sistema se asignan y se explican con suficiente detalle para proporcionar criterios de diseño y verificación para apoyar el diseño del sistema integrado".*[34]

Finalmente, Buede indica que *"el proceso de diseño de un sistema tiene que considerar más que el lado físico del mismo; las funciones o actividades que el sistema tiene que realizar son un elemento crítico para que el proceso de diseño tenga éxito de manera consistente".*[35]

Por último, la síntesis de diseño es definida por el Departamento de Defensa de Estados Unidos como *"el proceso mediante el cual los conceptos o diseños se desarrollan sobre la base de las descripciones funcionales que son los productos de análisis funcional y asignación; es una actividad creativa que desarrolla una arquitectura física".*[36]

Blanchard, en tanto, afirma que *"cuando se dispone de la suficiente definición y descomposición funcional, la síntesis se utiliza para definir aún más los CÓMO, en respuesta a los QUÉ del análisis funcional".*[37]

Uno de los elementos más importantes de la ingeniería de sistemas es representar la arquitectura del sistema y determinar la estructura y las relaciones entre el hardware, las comunicaciones, las operaciones, etcétera. Esto lo podemos ver en la síntesis a través de la descomposición y proceso de diseño bien elaborado. Según MITRE,[38] una vez que los requisitos se expresan y se doblan en un proceso de gestión, se puede describir una arquitectura de sistema. La arquitectura será la base para el desarrollo, la integración, las pruebas, el funcionamiento, la interconexión y la mejora del sistema a lo largo del tiempo.

En los artículos de arquitectura de sistemas, se discuten varios patrones de arquitectura (por ejemplo, arquitectura orientada a servicios) y marcos de arquitectura (tales como DODAF, marco de arquitectura y procesos formales para desarrollar arquitecturas). Según la NASA,[39] al igual que otros elementos de la descomposición funcional, el desarrollo de una a nivel de sistema es un proceso creativo, recursivo e iterativo que combina una excelente comprensión de los objetivos y limitaciones del proyecto con un conocimiento igualmente bueno de varios medios técnicos potenciales de entregar los productos finales.

---

34 Department of Defense United State of America (2001). *Op. cit.*, p. 45. Trad. del autor.
35 BUEDE, Dennis. *Op. cit.*, p. 211. Trad. del autor.
36 Department of Defense United State of America (2001). *Op. cit.*, p. 57. Trad. del autor.
37 BLANCHARD, *op. cit.*, 1995, p. 58. Trad. del autor.
38 MITRE (2014). *Op. cit.*, p. 272. Trad. del autor.
39 NASA (2007). Systems Engineering Handbook. Washigton: Nasa Headquarters, p. 50. Trad. del autor.

Hay varias herramientas que se pueden utilizar para desarrollar la arquitectura de un sistema. Estas son principalmente herramientas de modelado y simulación, herramientas de análisis funcional, marcos de arquitectura y estudios comerciales. Por ejemplo, una forma de hacer arquitectura es el Marco de Arquitectura del Departamento de Defensa (DODAF).

Para describir y caracterizar sistemas complejos y evolutivos, es necesario definir marcos de arquitecturas que sean entendidos por todos los que participan en los sistemas de sistemas, ya que esto permitirá la disminución de la complejidad. Estos marcos son útiles para asegurar que las necesidades de las partes interesadas sean claramente comprendidas.

Por lo anterior, NASA señala que el Departamento de Defensa de Estados Unidos *"ha establecido políticas que exigen el uso de la DODAF en la planificación de capital, la adquisición y la integración de capacidades conjuntas y define la arquitectura como la estructura de los componentes, sus relaciones y los principios y directrices que rigen su diseño y evolución a lo largo del tiempo".*[40]

Como afirma el Departamento de Defensa de Estados Unidos, *"hay tres perspectivas principales que se combinan lógicamente para describir una arquitectura. Estos tres puntos de vista de la arquitectura son las opiniones operacionales, de sistemas y técnicas"*, las cuales se pueden apreciar en la figura N° 3.[41]

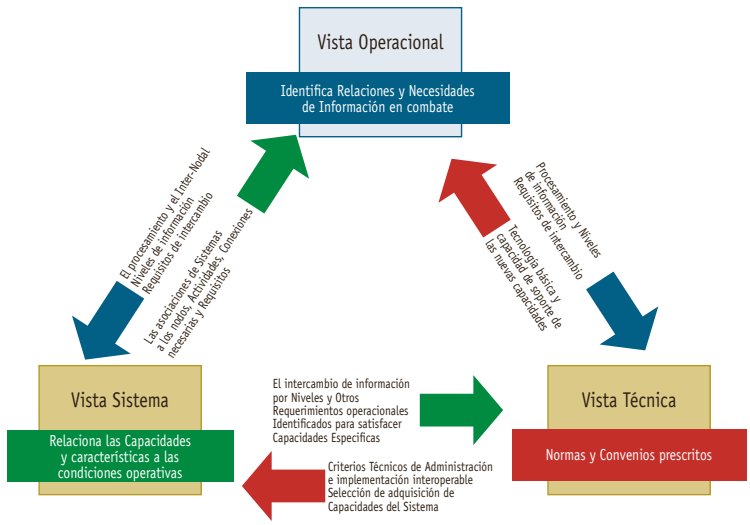


Figura N° 3: "Vínculos fundamentales entre las vistas de C4ISR Architecture Framework".

Fuente: Department of Defense United State of America C4ISR Architecture Framework, versión 2.0. C4ISR Architecture Working Group (AWG), 1997, p. 16.

40 *Ibídem*, p. 51. Trad. del autor.

41 Department of Defense United State of America (1997). C4ISR Architecture Framework version 2.0. C4ISR Architecture Working Group (AWG), p. 16. Trad. del autor.

DISEÑO DE ARQUITECTURA

Necesidades del sistema

Los primeros pasos para el diseño consisten en captar las necesidades, objetivos, requisitos y limitaciones que requieren las partes interesadas del sistema. En esta fase se requiere recopilar y aclarar todas las expectativas de todos los interesados en el diseño del sistema.

Para definir los requerimientos de las partes interesadas, se ha tomado como base el formato de documento de requerimientos operacionales (ORD),[42] el que proporciona un marco básico para la articulación y documentación de los requisitos operacionales.

Es definido por la Homeland Security como una "herramienta eficaz para transmitir las necesidades de un determinado componente, grupo o agencia en un formato fácilmente comprensible para evitar recursos desperdiciados y necesidades con poca claridad de interpretación".[43]

Además, consta de los siguientes puntos que son extractados para adquirir las necesidades de las partes interesadas: la descripción general de la capacidad operativa; la brecha de capacidad; la descripción general de la zona de la misión; la descripción del sistema propuesto; la misión que el sistema propuesto logrará; el concepto operativo y de soporte; la amenaza, insuficiencia del sistema existente; la capacidad requerida; los parámetros clave de rendimiento; el rendimiento del sistema y el soporte del sistema.

Para el presente *paper* se desarrollará solo la brecha de capacidad, debido a su importancia y concepto directivo de diseño. Con este fin se identificó la falta de capacidad de mando y control, que impide la visualización del panorama operacional común de los organismos desplegados en una catástrofe o desastre en sus respectivas zonas de empleo y las unidades en terreno.

Todo lo anterior con la finalidad de permitir el flujo de información en tiempo real en territorio nacional, asegurando la interoperabilidad y conectividad, con el objetivo de acelerar el ciclo de toma de decisiones.

---

42 HOMELAND SECURITY (2008). Developing Operational Requirements, a guide to the cost-effective and efficient communication of needs, p. 13. Washington: U.S. Department of Homeland Security Science and Technology Directorate. *ORD es el acrónimo de "Documento de Requerimientos Operacionales", este nombre será utilizado a partir de este punto. Trad. del autor.

43 *Ibídem*, p. 6. Trad. del autor.

Análisis de requerimientos

En el presente análisis de requerimientos, el producto deberá arrojar como resultado una comprensión clara de las funciones (lo que el sistema tiene que hacer), el desempeño (qué tan bien las funciones tienen que ser realizadas) y las restricciones (qué impide que se realicen las funciones).

Como ya se consignó, esta fase de diseño se centra en los "QUÉ" debe hacer el sistema y no en los "CÓMO". Algunos ejemplos de requerimientos son los siguientes:

Nº	REQUERIMIENTOS (ejemplos)	FUNCIÓN
1	El sistema debe ser capaz de transmitir órdenes	TRANSMITIR
2	El sistema debe ser capaz de recibir necesidades operacionales de los usuarios	RECIBIR
3	El sistema debe integrarse con una base de datos geográficos de todo el país	INTEGRAR
4	El sistema debe registrar información de todo el personal desplegado en la emergencia	REGISTRAR
5	El sistema debe comunicar la información entregada por los usuarios	COMUNICAR
6	El sistema debe ser capaz de visualizar las unidades que están desplegadas	VISUALIZAR
7	El sistema debe ser capaz de graficar el panorama de la catástrofe	GRAFICAR

Tabla Nº 1: "Ejemplos de requerimientos operacionales".

Fuente: Elaboración propia.

Una de las actividades más importantes del análisis de requerimientos es extraer las funciones de estos últimos, para utilizarlas en el siguiente paso de análisis funcional y en la fase de diseño, lo que se representa en detalle en la figura Nº 4.

Análisis funcional

En el presente *paper*, la arquitectura funcional será representada con un enfoque top-down (de arriba hacia abajo) de los requisitos funcionales.

La arquitectura mostrará solo la función de nivel superior y las funciones de primer nivel que las componen.

De esta forma, el método que será utilizado para representar la arquitectura funcional es IDEF0, donde, según Buede, *"una función o actividad está representada por una caja y descrita por una frase de verbo-sustantivo y numerada para proporcionar contexto dentro del modelo"*,[44]

44 DEPARTMENT OF DEFENSE UNITED STATE OF AMERICA (2001). *Op. cit.*, p. 51. Trad. del autor. *IDEF0 es capaz de representar gráficamente una amplia variedad de negocios, fabricación y otros tipos de operaciones empresariales a cualquier nivel de detalle. IDEF0 es el acrónimo de "Integration Definition for Function Modeling". Este nombre será utilizado a partir de este momento.

agregando que: *"una función en este contexto es una transformación que convierte entradas en salidas".*

Esto quiere decir que las entradas ingresan en la caja de funciones desde la izquierda hacia la derecha; por su parte, los controles que guían el proceso de transformación entran desde la parte superior; los mecanismos (recursos físicos que realizan la función) entran desde la parte inferior y las salidas emergen de la derecha.

El IDEF0 se utiliza para mostrar tanto el flujo de datos, el control del sistema y el flujo funcional de los procesos.

Para clarificar lo anterior, se presenta la figura N° 4 que asocia los niveles de un SMC en la GRD.

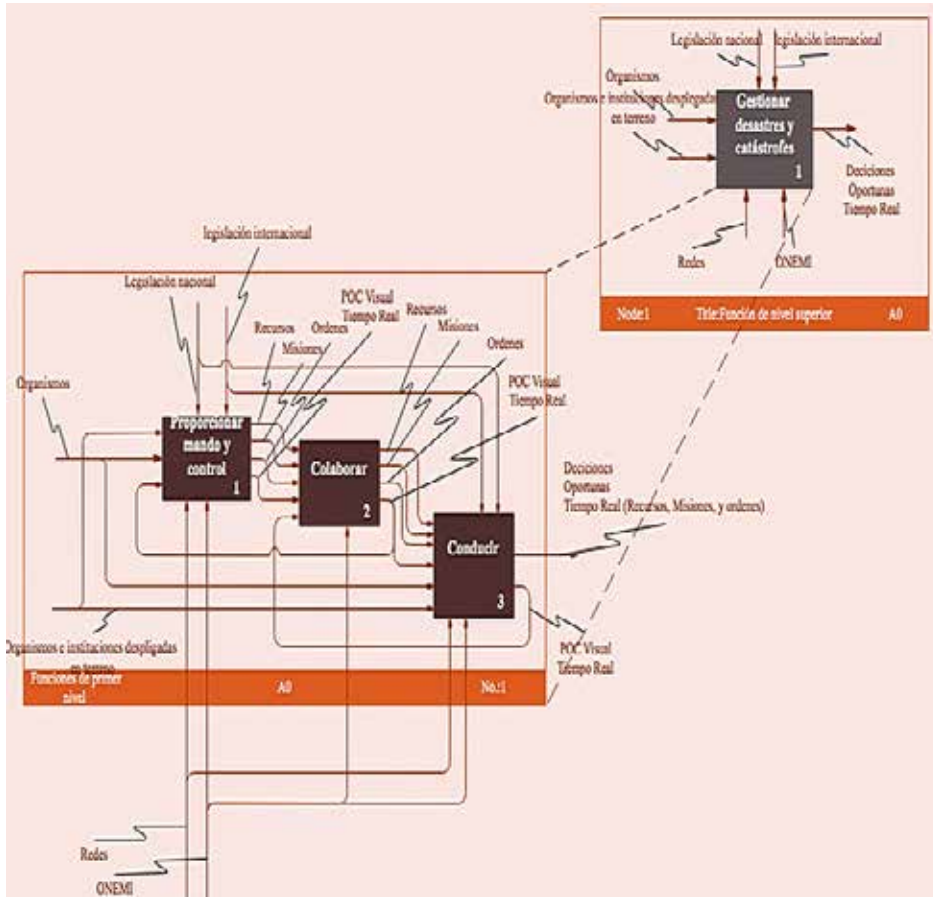


Figura N° 4: "Diagrama IDEF0".

Fuente: Elaboración propia.

Síntesis del diseño

La arquitectura física de un sistema es una descripción jerárquica de los recursos que componen el mismo.

Esta jerarquía comienza con los componentes de nivel superior del sistema y progresa hasta los elementos de configuración que comprenden cada componente intermedio.

Blanchard explica que la síntesis se utiliza *"en el desarrollo de conceptos para establecer las relaciones básicas entre los distintos componentes del sistema".*[45]

Más tarde, cuando se dispone de la suficiente definición y descomposición funcional, la síntesis se utiliza para definir aún más los CÓMO, en respuesta a los QUÉ del análisis funcional.

Otro producto que arroja el análisis de requerimientos se expresa desde una de tres perspectivas o vistas de la arquitectura Framework C4ISR del sistema, tal como se ha explicado en el presente *paper*.

A modo de ejemplo, se representará una vista operativa de alto nivel, denominada OV Nº 1, por sus siglas en inglés (Operational View), de acuerdo con la metodología DODAF, la que describirá la misión y el escenario.

Además, muestra los principales conceptos operativos y los aspectos interesantes o únicos de las operaciones, a la vez que describe las interacciones entre la arquitectura del sujeto y su entorno, y entre la arquitectura y los sistemas externos.

Como se puede apreciar, la OV Nº 1 proporciona una representación gráfica de todos los factores involucrados en el diseño de un sistema de mando y control.

Esta vista puede usarse para orientar y enfocar discusiones detalladas. Su principal uso es ayudar a la comunicación humana y está destinado a una presentación de alto nivel de la toma de decisiones.

45 BLANCHARD, *op. cit.,* p. 58.

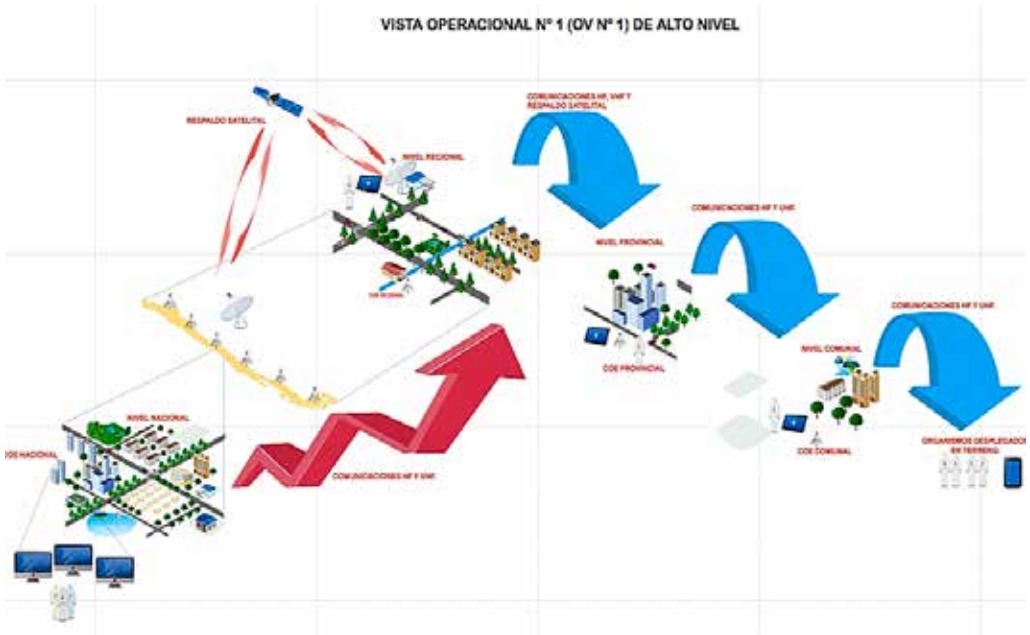


Figura N° 5: "Ejemplo de una vista operacional N° 1".

Fuente: Elaboración propia.

CONCLUSIONES

Todas las emergencias, desastres o catástrofes acontecidos en nuestro país nos han demostrado las importantes amenazas que estos eventos presentan para nuestra sociedad. El saber gestionarlos y mitigar los impactos es responsabilidad de todos los actores, tanto públicos como privados.

Dentro del ciclo de gestión del riesgo de desastres, es en la fase 2 –"Respuesta"– en donde, desde el punto de vista operacional, los sistemas de mando y control son fundamentales, con el objeto de adquirir una visión global de la situación mediante el intercambio de información y de la percepción de la situación.

En esta fase las situaciones son más complejas y dinámicas, por lo que requieren que los actores tomen decisiones óptimas bajo restricciones de alto riesgo, incertidumbre, alta carga de trabajo y presión de tiempo.

Por esta razón, este *paper* se enfocó en la importancia de la metodología para el diseño de las arquitecturas de mando y control que le permita al Sistema Nacional de Protección Civil (SNPC) aumentar la "conciencia situacional" para la toma de decisiones, en las acciones de respuesta en las distintas fases operativas ante situaciones de emergencia, desastre o catástrofe.

BIBLIOGRAFÍA

ALBERTS, D. S. & HAYES, R. E. (2006). *Understanding command and control,* Washington, DC., Estados Unidos, CCRP.

ALBERTS, D. S.; GARSTKA, J. J. & STEIN, F. P. (2005). 2ª edición. *Network centric warfare: Developing and leveraging information superiority,* Washington, DC., Estados Unidos, CCRP.

ARNOLD, Ross y WADE, Jon (2015). *A Definition of Systems Thinking: A Systems Approach,* (en línea). Nueva York: Elsevier B.V.

ARROYO de la Rosa, Rodolfo (2014). "Las transmisiones militares en emergencias: un terreno nada desconocido". *Revista Ejército de Tierra de España*.

BREHMER, Berndt (2006). *The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control.* Stockholm: Department of War Studies Swedish National Defence College.

BUEDE, Dennis (2009). *The Engineering Design of System, Models and Methods,* New Jersey: A John Wiley & Sons.

BLANCHARD, Benjamín (1995). *Ingeniería de Sistemas.* Madrid: Isdefe.

CHUMER, Michael y Turoff, Murray (2005). *Command and control (C2): Adapting the distributed military model for emergency response and emergency management,* (en línea). New Jersey: New Jersey Institute of technology.

Consejo Nacional de Innovación para el Desarrollo. Hacia un Chile Resiliente frente a desastres: Una oportunidad, (en línea). Santiago de Chile, 2016 p. 14. Disponible a través de http://www.cnid.cl/wp-content/uploads/2016/12/CREDEN-27122016-2.pdf

Department of Defense United State of America (2001). *Systems engineering fundamentals.* Virginia: Supplementary text prepared by the defense acquisition University press Fort Belvoir.

Department of Defense United State of America (1998). *Levels of information system interoperability (LISI).* Architecture Working Group (AWG).

Department of Defense United State of America (1997). *C4ISR architecture framework (2.0 ed.).* Architecture Working Group (AWG).

Department of Defense United State of America (1974). *Military Engineering Standard Management*. Washington: Air Force Sytems Command.

ESTEVE, Manuel (2016). *C4ISR Multimedia System for Emergency Management TIN2004-03588,* (en línea). Valencia, Departamento de Comunicaciones Universidad Politécnica de Valencia.

GREEN, W. G. (2001). *Command and control of disaster operations*. Boca Ratón, FL., Estados Unidos, Universal publishers.

HOMELAND Security (2008). *Developing operational requeriment, a guide to the cost-effective and efficient communication of needs*. 2.0. Washington: U.S. Department of Homeland Security Science and Technology Directorate.

International Council on Systems Engineering (INCOSE) (2003). *Systems Engineering Handbook a Guide for System Life Cycle Processes and Activities*. San Diego: Cecilia Haskins.

JOBIDON, Marie Eve; LABRECQUE, Alexandre; TURCOTTE, Isabelle; ROUSSEAU, Vincent y TREMBLAY, Sébastien (2007). *Adaptability in Crisis Management: The Role of Organizational Structure,* (en línea). Toronto: Defence R&D.

MEISSNER, Andreas; LUCKENBACH, Thomas; RISSE, Thomas; KIRSTE, Thomas y KIRCHNER, Holger (2002). *Design Challenges for an Integrated Disaster Management Communication and Information System,* (en línea). Berlín: Institute for Open Communication Systems.

Ministerio del Interior y Seguridad Pública (2002). Plan Nacional de Protección Civil, Decreto N° 156, 2002. Santiago de Chile: ONEMI.

Ministerio del Interior y Seguridad Pública (2015). Plan Estratégico Nacional para la Gestión del Riesgo de Desastres 2015-2018. Santiago de Chile: ONEMI.

Ministerio del Interior y Seguridad Pública (2017). Plan Nacional de Emergencia. Santiago de Chile: ONEMI.

MITRE (2014). *Systems Engineering Guide*. The MITRE Corporate Communications and Public Affairs.

NASA (2007). *Systems Engineering Handbook*. Washington: NASA Headquarters.

OGASAWARA, Junji; TANIMOTO, Koichi; IMAICHI, Osamu y YOSHIMOTO, Masayoshi (2014). Disaster Prevention and Response Support Solutions, (en línea). Hitachi Review.

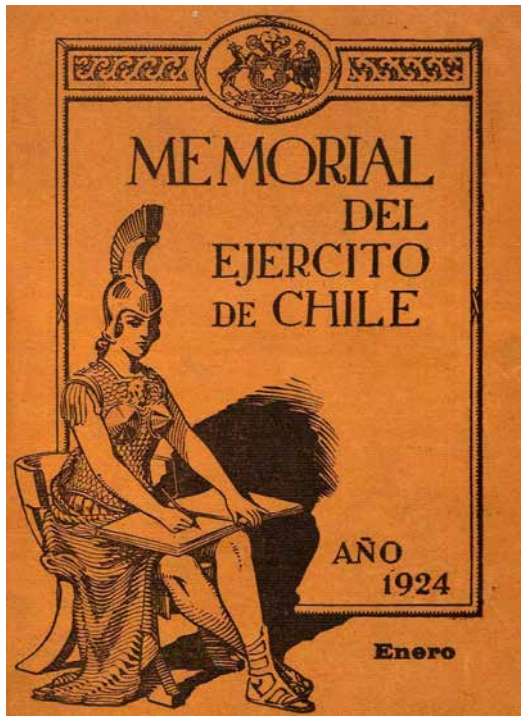
OSINGA, Frans (2005). *Science, Strategy and War The Strategic Theory of John Boyd*. Amsterdam: Eburon Academic Publishers, (en línea).

SENGE, Peter (1990). *The Fifth Discipline, The Art and Practice of the Learning Organization*. New York: Doubleday/Currency.

TOOD, David; TOOD, Hazel (2011). Natural disaster response, independent evaluation group, (en línea). Washington, DC.: World Bank.

United Nations (en línea). Marco Sendai para la reducción del riesgo de desastres (2015-2030), disponible a través de: https://www.unisdr.org/files/43291_ spanishsendaiframeworkfor-disasterri.pdf

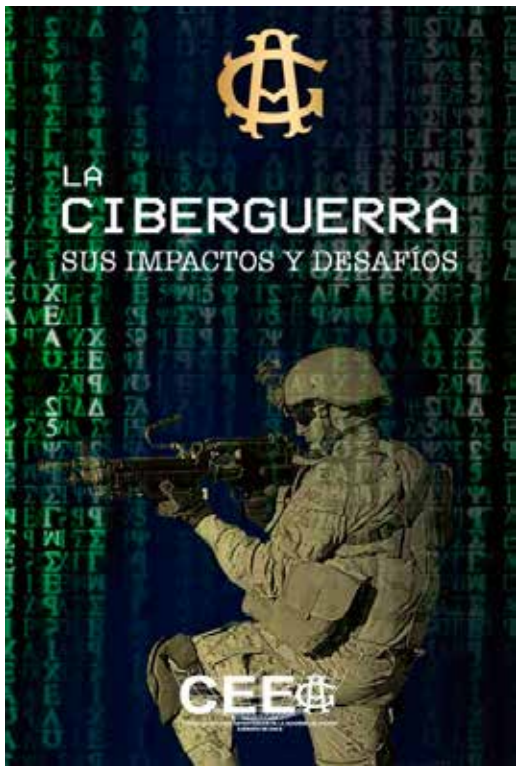
COMENTARIOS DE LIBROS Y REVISTAS MILITARES



MEMORIAL
DEL
Ejército de Chile

LA CIBERGUERRA: SUS IMPACTOS Y DESAFÍOS

AUTORES: GDD (R) MARIO ARTEAGA VELÁSQUEZ – GDB (R) RENÉ LEYVA VILLAGRA - CRL. (R) CARL MAROWSKI PILOWSKY – CRL. (R) HERNÁN DÍAZ MARDONES – TCL. (R) MARIO POLLONI CONTARDO
COMENTARIO: MAY. (R) FELIPE AMAR TOBAR[1]



La ciberguerra, sus impactos y desafíos es el resultado del Tema de Investigación Central de la Academia de Guerra (TICA) correspondiente al período 2016-2017, que contempló un trabajo colaborativo, donde resalta la innovación, con aportes de conocimiento estratégico en un área donde había que explorar mucho e investigar en profundidad.

Sus autores fueron dando vida a las respuestas conducentes a satisfacer una interrogante principal: ¿cuáles son los impactos que la ciberguerra puede tener en la infraestructura crítica nacional y qué aportes se pueden hacer en ello a fin de sustentar una estrategia de disuasión en ciberguerra encuadrada en las normativas vigentes?

Capítulo I: haciendo referencia a los diferentes componentes conceptuales y constituyentes de la ciberguerra, el autor del capítulo expone las diferentes implicancias de los procesos de ciberoperaciones, así como también del ciberespacio y los sistemas de mando y control, tomando como referencia que su complejidad también es de tipo doctrinario al no ser definido por esta, siendo necesario una reflexión en torno a este punto.

Capítulo II: el autor nos presenta un análisis respecto a la necesidad de establecer la relación entre la ciberguerra y las infraestructuras críticas, visualizando cuáles de estas pueden tener una mayor vulnerabilidad a las acciones de la ciberguerra, tomando como referencia a los principales

1 Asesor del Sistema de Investigación y Desarrollo del Ejército. Centro de Estudios e Investigaciones Militares.

actores del mundo en el tema, como lo son Estados Unidos y Europa, particularmente el caso de España y las acciones que ha establecido para enfrentar este fenómeno.

Capítulo III: comenzando desde la interrogante: ¿de qué manera se relaciona la ciberguerra con la disuasión?, y existiendo para el autor una línea que relaciona a ambos elementos desde el entendimiento de las amenazas, se configuran ideas de acción sobre la base de articular el arte de la estrategia con la tecnología de lo cibernético y sus consideraciones con el área de la defensa.

Capítulo IV: estableciendo que existe una relación entre ciberguerra, guerra de información, mando y control, y ciberespacio, en este capítulo se advierte que es necesario investigar y reflexionar con respecto al combate por el mando y control, de tal manera que sea posible identificar los factores que intervienen, las amenazas que puedan afectarle y las condiciones y desafíos para alcanzar la victoria.

Capítulo V: con la primicia de que la infraestructura crítica de una nación puede ser sujeta de ataques cibernéticos por parte de grupos internacionales, de individuos provenientes desde otro Estado o desde el interior de la propia nación, trata sobre la amenaza para la estructura nacional de carácter sensible, considerando la correspondiente defensa nacional, la de sus instituciones y la perteneciente a las organizaciones que las apoyan y contribuyen a su sostenimiento.

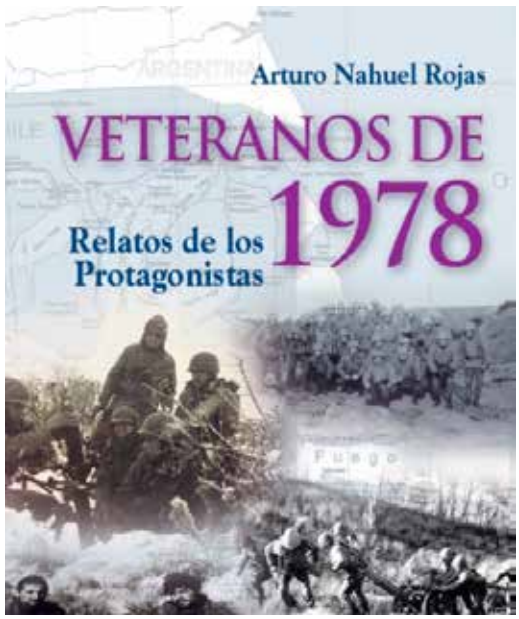
Capítulo VI: el autor presenta una síntesis de cómo el Derecho Internacional regula las acciones desarrolladas por diversos actores en el marco de la llamada "ciberguerra", para ello desarrolla un concepto distintivo de la ciberguerra, coincidiendo con autores anteriores a pesar de la diferencia de parámetros y de una naturaleza distinta.

Capítulo VII: los autores plantean una serie de desafíos que se deben considerar al afrontar una ciberguerra, adoptando una perspectiva regional y enfocándose en las herramientas utilizadas, entre ellas, la CESIRT y sus diferentes utilidades.

Reflexiones finales: los autores realizan una síntesis de los principales planteamientos del libro, tomando en consideración sus implicancias a futuro; de igual forma se refieren al aumento del número de estudios sobre la ciberguerra, en donde la generación de nuevo conocimiento estratégico será necesaria, particularmente en el ámbito de la disuasión y el combate por el mando y control.

VETERANOS DE 1978. RELATOS DE LOS PROTAGONISTAS

AUTOR: ARTURO NAHUEL ROJAS
COMENTARIO: PAC. FRANCISCO SÁNCHEZ URRA[1]



Muchas veces la historia como disciplina nos pone en la disyuntiva de que las fuentes, elemento esencial y fundamental para el trabajo de investigación, son mudas e inexpresivas, generando la especulación del historiador en tratar de deducir el contexto, complicando, en ocasiones en forma inexorable, la comprensión de las pasiones de la época de estudio y la tarea de establecer un verdadero entendimiento del devenir de las personas en tiempos y zonas geográficas enmarcados por procesos que, al fin y al cabo, nos permiten comprender los hechos que se han desarrollado en la historia.

El presente libro tiene una ventaja extraordinaria en relación a otros estudios que se han realizado en una temática tan apasionante como es la crisis con Argentina de 1978, momento que es parte de un proceso mucho más amplio y complejo (que algunos autores hemos tratado como una coyuntura entre 1977 a 1984 al menos), esta radica en el haber podido acceder a parte de las "fuentes vivas" que ha dejado la crisis de 1978, y años posteriores, pudiendo el investigador en efecto "dialogar con las fuentes", comunicar sus sentimientos a 40 años de los sucesos y comprender, sintetizar y transmitir de qué forma diferentes actores, al día de hoy, van nutriendo estudios estrictamente jurídicos o documentales, dando vida a un contexto lleno de pasión, angustia, miedos y alegrías, pero cruzado por una firme convicción en la justa causa que llevó a miles de chilenos a ser desplazados a distintos rincones de la frontera y a otros a colaborar en el inmenso esfuerzo de la defensa de nuestra patria ante la eventual agresión, que, por críticos períodos, pareció inevitable.

1 Asesor del Sistema de Investigación y Desarrollo del Ejército. Centro de Estudios e Investigaciones Militares.

Se logra configurar un interesante panorama en torno a los diferentes procesos que se llevan a cabo en el período en estudio, aplicando una interesante metodología y estableciendo un marco conceptual que es un aporte, pocas veces logrado por otros estudios en relación al período, en torno a la problemática en cuestión y las singularidades que el proceso de "la Crisis del Beagle" conllevó.

Es de esta manera que en parte logra ser un aporte al debate y sobre todo a la labor esencial del historiador que es en sí difundir a quienes, sin necesaria formación, buscan conocer y comprender los diferentes acontecimientos que rodean un estudio de esta envergadura. Es de esta forma que el autor, en una pluma y lenguaje amplio, logra transmitir la esencia de su estudio y conocimiento, el cual es fruto de la investigación realizada, brindando no tan solo un texto atractivo sino una importante fuente de consulta para los historiadores que, por motivo del paso del tiempo y la naturaleza humana, no podrán acceder a las "voces y sentimientos" de algunos protagonistas en los próximos años.

El presente libro es, sin lugar a dudas, un homenaje a aquellos que, en diferentes sectores de la frontera y apoyando otros a las fuerzas desplegadas, al igual que en el campo político y diplomático, tanto civiles como militares, configuraron uno de los hechos más importantes de nuestra historia patria reciente, en donde se cruzan miles de relatos, algunos callados por el tiempo, pero que fueron participes de la disuasión y establecimiento de la paz entre dos países que tienen una larga historia en común, paz que, en el contexto en estudio, fue forjado con sacrificio y entrega, valentía y desvelos, miedos y angustias, pero legándonos una herencia trascendente para recordar: que cuando la patria es amenazada, se superan transitorias diferencias políticas, sociales y enemistades, siendo un ejemplo de la manera en que los valores trascendentes tienen que ser fortalecidos cada día y mostrándonos el orgullo que debemos sentir por cientos de miles que nos han legado un Chile en paz y progreso.

Debemos recordar que la historia como disciplina es el reflejo de la libertad de las personas en su tiempo, su espacio e ideas, sobre esta base se van conformando procesos de análisis, reflexiones que nos dan una comprensión del proceso y la generación de una visión y sentir respecto al pasado, elementos que van conformando un relato para aquellos que, con distancia e interés, buscan un punto de partida para la comprensión del pasado y su relevancia en el presente.

El leer y releer el presente libro es una oportunidad para escuchar las voces de aquellos que vivieron y sintieron los "vientos ensordecedores de la guerra" y que, pasados los años, hoy en paz, nos logran transportar a aquellos duros momentos, haciéndonos sentir un profundo orgullo por su labor, que esperemos algún día cuente con el espacio merecido en nuestra historiografía y con el homenaje de toda una nación.

NORMAS EDITORIALES

MEMORIAL
DEL
Ejército de Chile

NORMAS EDITORIALES

La revista *Memorial del Ejército de Chile* es la publicación más antigua de la institución. Creada el 15 de julio de 1906, desde esa fecha se ha posicionado como un medio de difusión de las inquietudes profesionales de las distintas generaciones de oficiales, con el propósito de profundizar temáticas relacionadas con la profesión y su entorno, contribuyendo al debate de ideas y a la generación de conocimiento.

A contar del año 2015, su elaboración y publicación la asumió el Centro de Estudios e Investigaciones Militares (CESIM), que también se encarga de su distribución semestral a las entidades académicas, centros de estudios nacionales y extranjeros, Fuerzas Armadas, de Orden y Seguridad e investigadores, entre otros.

El contenido de cada una de las ediciones está basado en artículos relacionados con las ciencias militares, abordando las distintas dimensiones que inciden en la profesión militar. También se elaboran ediciones temáticas, en las que se centran los primeros artículos, sin dejar de considerar otros tópicos de diversa naturaleza, monografías y ensayos, en el marco de la línea editorial previamente establecida, difundida, además, en la página web del CESIM: www.cesim.cl en el link "publicaciones".

Aquellas personas que quieran colaborar pueden remitir sus escritos a memorialdelejercito.cesim@ejercito.cl, o bien al correo intranet institucional A1005, cumpliendo con las siguientes normas:

Artículos: estos deben tener una extensión máxima de 9.000 palabras, aproximadamente, escritas en letra Arial 12, a 1,5 de espacio y deben ser inéditos. Si el trabajo es el resultado de una ponencia o producto de alguna investigación, deberá puntualizarse mediante un asterisco, colocado al final del título y que remita a una primera nota a pie de página. En caso de utilizarse cuadros, gráficos o mapas, deberá explicitarse su fuente.

Todos los artículos deben contener un breve currículum del autor (grados académicos, pertenencia a alguna institución y e-mail) en nota a pie de página.

Además, el artículo debe contener un **resumen** de no más de 100 palabras y su traducción al inglés (abstract), así como señalar cinco **palabras clave**, en ambos idiomas, que representen la temática que aborda el escrito.

En relación a las **referencias bibliográficas**, deberán ser enumeradas consecutivamente y estar al pie de página, de acuerdo al International Standarization Organization (ISO). En función del manual de referencias, el orden para citar los textos es el siguiente:

- Autor
- Título de la publicación
- Lugar de la publicación
- Casa editorial
- Año de la edición
- Número de página

Ejemplo de libro: WILHELMY, Manfred. Política Internacional: Enfoques y Realidades, Buenos Aires, Argentina, Grupo Editor Latinoamericano, 1988, p. 45.

En el caso de los artículos contenidos en revistas impresas, deben citarse de acuerdo al siguiente orden:

- Autor del artículo
- Título del artículo
- Título de la revista en letra cursiva o subrayada
- Volumen si lo incluye la revista
- Número de la edición (anotar entre paréntesis)
- Número de página (precedida de 2 puntos)
- Fecha de la edición (indicar mes y año)

Ejemplo de artículo: FERRADA, Luis. "La defensa nacional y su aporte a la política antártica de Chile", *Escenarios Actuales* (N° 3) p. 29, diciembre 2012.

Si el texto referido no corresponde a un artículo o libro, se debe especificar la fuente (Ej: caso de monografía electrónica). En tal caso la referencia completa se debe ordenar así:

- Responsabilidad principal
- Título
- Tipo de soporte
- Edición
- Lugar de publicación
- Casa editorial
- Fecha de edición
- Fecha de actualización / revisión
- Disponibilidad y acceso (obligatorio para documentos en línea)
- Número normalizado.

Ejemplo de referencia electrónica: -Kirk-Othmer Encyclopedia of Chemical Technology (en línea). 3rd ed. New York: John Wiley, 1984 (citado 3 de enero 1990) disponible a través de: DIALOG Information Services, Palo Alto (Calif.).

La **Bibliografía** completa deberá ser proporcionada al final del trabajo, en orden alfabético de los apellidos de los autores.

Ejemplo de libro: WILHELMY, Manfred (1998). Política Internacional: Enfoques Realidades, Buenos Aires, Argentina, Grupo Editor Latinoamericano.

CENTRO DE ESTUDIOS E INVESTIGACIONES MILITARES
CESIM

IGM TALLERES GRÁFICOS