ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TÍTULO: Las características del criterio de modularidad en el diseño de un elemento de comunicaciones, guerra electrónica y ciberdefensa en el ámbito de las operaciones multidominio en la actualidad.

AUTOR: MY EA RODRIGO LUCAS OVIEDO

TUTOR: TC DIEGO ALEJANDRO PARIENTE

AÑO: 2024

Resumen

La legislación Argentina referente a la defensa nacional establece estrictos lineamientos para regular las actividades relacionadas con las comunicaciones, guerra electrónica y ciberdefensa. La Ley de Defensa Nacional (Nro. 23554) y su reglamentación (Decreto 727/2006) delimitan las fuerzas armadas que solo pueden intervenir en respuesta a agresiones externas, requiriendo la previa declaración de un teatro de operaciones para llevar a cabo actividades militares completas.

La estrategia de defensa de restricción de área se ejecuta dentro de un marco legal que restringe las operaciones de guerra electrónica y ciberdefensa en tiempos de paz, garantizando la conformidad con las normativas nacionales y la disposición para una rápida activación en caso de conflicto declarado.

Esta estrategia demanda a las fuerzas armadas ciertas características, como la modularidad, que posibilita una respuesta flexible y coordinada, integrando capacidades en múltiples dominios y aprovechando tecnologías avanzadas para operaciones multidominio.

El sistema de comunicaciones a nivel operacional debe cumplir con los requisitos para conformar organizaciones militares que sean flexibles, interoperables, modulares y sostenibles, facilitando la conducción de operaciones multidominio por parte del comandante, y permitiendo aprovechar las oportunidades que se presenten.

A través del análisis de la legislación argentina, la doctrina militar vigente y publicaciones sobre modularidad en el ámbito civil y militar, se plantea como objetivo principal analizar las características modulares que debería reunir un elemento de comunicaciones, guerra electrónica y ciberdefensa para favorecer la conducción de un comandante en operaciones multidominio articuladas con el plexo legal.

Se determinaron los siguientes lineamientos para el abordaje de la temática; estudio pormenorizado del estado del arte actual; análisis comparado de la legislación nacional vigente y la estrategia de defensa nacional; y análisis del modelo de ingeniería en sistemas sobre las características modulares. Estos aspectos limitados a los elementos de comunicaciones, guerra electrónica y ciberdefensa para su aplicación en el nivel operacional.

Palabras clave: Modularidad – Multidominio – Comunicaciones – Guerra Electrónica – Ciberdefensa

Índice

Introducción

El presente trabajo se centra en la modularidad de los sistemas de comunicaciones, guerra electrónica y ciberdefensa, en el contexto de operaciones multidominio, articulándolos con la legislación nacional vigente.

Los análisis realizados sobre la doctrina militar conjunta, como específica de cada componente de las fuerzas armadas argentinas, se reconoció que existen aspectos ausentes relacionados al criterio de modularidad y sus características, las que debieran reunir las organizaciones militares vinculadas a la estrategia de defensa nacional y a la legislación vigente.

La doctrina militar conjunta de las fuerzas armadas argentinas establece las situaciones en las cuales las organizaciones se estructuran bajo las premisas de los criterios organizacionales con capacidades adaptables al entorno. Las doctrinas específicas de los componentes terrestre, aéreo y naval se encuentran brevemente mencionadas y descriptas.

De lo expuesto anteriormente, se han efectuado trabajos relacionados a lograr ciertos criterios organizacionales, como la flexibilidad y la interoperabilidad. Entre esos trabajos podemos mencionar el de la Mayor Paulina Soledad Policante en la Escuela Superior de Guerra en 2021, titulado "Diseño de un Sistema de Comunicaciones Interoperable para el Instrumento Militar de la Nación". El cual se centraba en la necesidad de diseñar un sistema de comunicaciones que garantice la interoperabilidad del instrumento militar de la nación durante la paz, facilitando el adiestramiento conjunto para garantizar eficiencia en la comunicación durante conflictos.

En la misma línea, está el trabajo realizado por el Mayor Francisco Javier Baigorria en la Escuela Superior de Guerra Conjunta en 2019, titulado “Estructura del Sistema de comando y Control en el Nivel Operacional y los desafíos del siglo XXI”. Esta investigación tuvo como objetivo establecer los lineamientos fundamentales que debe contener el sistema de comando y control en el nivel operacional de la República Argentina, permitiéndole enfrentar los desafíos del siglo XXI en un teatro de operaciones. Estos lineamientos se enfocaron en la estructuración del sistema de comando y control, considerando características esenciales como la integración, flexibilidad, movilidad, resiliencia e interoperabilidad, así como la capacidad de incorporar tecnología de inteligencia artificial.

Otro estudio relevante es el Trabajo Final de Licenciatura desarrollado por el

Mayor Alejandro Oscar Ratti en la Escuela Superior de Guerra en 2011, titulado "Interoperabilidad de los sistemas de comunicaciones en apoyo al comando y control en el nivel estratégico operacional". Este estudio buscaba determinar las facilidades de comunicaciones adecuadas para lograr la interoperabilidad entre la fuerza aérea y el ejército en un teatro de operaciones.

Dentro de la línea de investigación de la ciberdefensa y del criterio para conformar organizaciones de interoperabilidad se encuentra el Trabajo Final Integrador desarrollado por el Mayor Luis Javier Anca en la Escuela Superior de Guerra Conjunta en 2015, titulado “La ciberdefensa: hacia el desarrollo de una interoperabilidad conjunta del teatro de operaciones”. El objetivo de este estudio era analizar la ciberdefensa relacionada con la conducción en el teatro de operaciones, para identificar los principios de la guerra que el comandante debe aplicar para lograr una interoperabilidad conjunta. Con ello, el autor interpreta el ambiente donde se llevan a cabo las operaciones de ciberdefensa y luego, vincula las operaciones de defensa cibernética en el nivel operacional.

En otra línea de investigación relacionad a la guerra electrónica se encuentra el Trabajo Final Integrador desarrollado por el Capitán de Corbeta Anselmo Omar Herrera en la Escuela Superior de Guerra Conjunta en 2015, titulado “Diseño y planificación de las actividades de guerra electrónica en el ambiente operacional”. Este estudio buscaba explicar las actividades de guerra electrónica que se realizan en el diseño de la campaña, enumerando las tareas de guerra electrónica en apoyo a las actividades de obtención de información, determinando la interoperabilidad necesaria para actualizar la librería de guerra electrónica conjunta, analizando la utilización de los medios de guerra electrónica de las fuerzas armadas para su empleo dentro de un comando conjunto.

Los trabajos encontrados están relacionados, en su mayoría, con la interoperabilidad y las condiciones necesarias para lograrla a nivel operacional, siendo esta una de las condiciones para alcanzar la modularidad.

Como resultado del proceso de investigación realizado, se encuentran vacíos concernientes a las características modulares que determinan a una organización militar, en este caso en un sistema de comunicaciones, guerra electrónica y ciberdefensa. Asimismo, este concepto está relacionado a la estrategia de defensa nacional de restricción aérea, implementada mediante las operaciones multidominio.

El estado actual del tema permitió reconocer, sobre los análisis realizados

sobre la doctrina militar conjunta, como específica de cada componente de las fuerzas armadas argentinas, que existen aspectos ausentes relacionados al criterio de modularidad y sus características, las que debieran reunir las organizaciones militares vinculadas a la estrategia de defensa nacional y a la legislación vigente. Esto último, tiene sus implicancias en cuanto a los alcances y limitaciones en las actividades de comunicaciones, guerra electrónica y ciberdefensa.

Con la elaboración de este trabajo de investigación se pretende contribuir; mediante el estudio pormenorizado del estado del arte actual y el análisis comparado de la legislación nacional vigente, la estrategia de defensa nacional, las publicaciones militares de países extranjeros relacionados a la temática, y el modelo de ingeniería en sistemas, con las características modulares que es ineludible que reúnan los elementos de comunicaciones, guerra electrónica y ciberdefensa.

Además, aportar las bases para una actualización a la doctrina militar del nivel operacional, favorecer a la ampliación del tema abordado a los ámbitos específicos de las fuerzas armadas y facilitar los fundamentos sobre su diseño, contribuyentes a la conducción de las operaciones multidominio en la actualidad.

Se limitará exclusivamente al nivel operacional para aplicar las características mencionadas sobre un elemento de comunicaciones, guerra electrónica y ciberdefensa, que contribuyan a la conducción del comandante en operaciones multidominio aprovechando las oportunidades inesperadas de acuerdo con la legislación vigente.

A fin de afrontar lo anteriormente descripto, surge el siguiente interrogante que guía esta investigación: ¿cuáles son las características modulares que deberá reunir un elemento de comunicaciones, guerra electrónica y ciberdefensa para favorecer la conducción de un comandante en las operaciones multidominio? Con el objetivo general de analizar las características modulares de un elemento de comunicaciones, guerra electrónica y ciberdefensa en las operaciones multidominio articuladas con la legislación nacional vigente. Estableciendo como supuesto: las características modulares de un elemento de comunicaciones, guerra electrónica y ciberdefensa favorecen la conducción de un comandante en las operaciones multidominio.

Por lo expuesto, para alcanzar dicho propósito, los objetivos específicos se centran en analizar las actividades de comunicaciones, guerra electrónica y ciberdefensa a desarrollar en las operaciones multidominio a la luz de la legislación argentina vigente e, identificar las características modulares para conformar un elemento de comunicaciones, guerra electrónica y ciberdefensa.

La presente investigación será descriptiva, a través de una metodología cualitativa. Se recurrirá a fuentes secundarias con el análisis bibliográfico y documental. En la fase inicial se reunirá bibliografía civil y militar, así como también trabajos académicos aprobados de alumnos y profesores que han desempeñado actividades en la Escuela Superior de Guerra Conjunta, sobre la temática abordada.

Posteriormente, se efectuará el análisis de la legislación nacional en materia de defensa, la doctrina específica y conjunta vigente en Argentina, obteniendo conclusiones parciales sobre su vinculación con la investigación.

En una tercera fase, con la bibliografía y artículos de revistas especializadas relacionadas con la disciplina de ingeniería en sistemas, se analizarán los aspectos que hacen al criterio de modularidad y su vinculación con los sistemas de comunicaciones, guerra electrónica y ciberdefensa para las operaciones multidominio en la actualidad.

En el presente trabajo, se aborda un análisis exhaustivo de las actividades relacionadas con las comunicaciones, la guerra electrónica y la ciberdefensa, en el contexto de la legislación nacional vigente y la estrategia nacional de defensa. En el primer capítulo, se examinan las limitaciones, restricciones y congruencias de estas actividades, evaluando cómo se alinean con el marco legal y estratégico del país.

El segundo capítulo se centra en identificar las características modulares de estos ámbitos dentro del entorno militar. Para ello, se realiza un análisis comparativo de la doctrina militar extranjera y de diversas publicaciones, tanto civiles como militares, sobre la modularidad en las organizaciones y sistemas. Finalmente, se presenta un aporte personal en el que se determinan las características modulares específicas de las organizaciones involucradas en estos campos, destacando su relevancia y aplicabilidad.

Capítulo 1. Las actividades de comunicaciones, guerra electrónica y ciberdefensa vinculadas con la legislación nacional vigente y la estrategia nacional de defensa

1. Aspectos generales de la legislación nacional Argentina

Para abordar la legislación nacional Argentina en relación con la defensa y seguridad, específicamente en actividades de comunicaciones, guerra electrónica y ciberdefensa, se deben considerar diversas normativas que establecen el marco legal en estas áreas. Las que se encuentran son:

1.1. Ley de Defensa Nacional (Nro. 23554): establece los principios y las normas fundamentales que regulan la defensa nacional en Argentina, incluyendo aspectos relacionados con las comunicaciones y la guerra electrónica[1].

1.2. Ley de Seguridad Interior (Nro. 24059): complementa la Ley de Defensa Nacional y aborda aspectos específicos de la seguridad interior, incluyendo las comunicaciones en contextos de seguridad y defensa[2].

1.3. Ley de Protección de los Datos Personales (Nro. 25326): es crucial en el ámbito de la ciberdefensa. Esta ley regula el tratamiento de datos personales y establece derechos y obligaciones que deben ser considerados en las operaciones de ciberdefensa[3].

1.4. Decreto Nº 727/2006: reglamenta la Ley de Defensa Nacional, especificando las competencias y responsabilidades de las fuerzas armadas, incluyendo las áreas de comunicaciones y guerra electrónica[4].

1.5. Estrategia Nacional de Ciberdefensa: aunque no es una ley, la Estrategia Nacional de Ciberdefensa proporciona una visión integral y directrices específicas para la protección de infraestructuras críticas y la respuesta a amenazas cibernéticas, abarcando aspectos de ciberdefensa[5].

---

[1] República Argentina; Ley de Defensa Nacional, Nro. 23554; sancionada el 13 de abril de 1988, promulgada el 26 de abril de 1988; Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-23554-28646.

[2] República Argentina; Ley de Seguridad Interior, Nro. 24059; sancionada el 18 de diciembre de 1991, promulgada el 6 de enero de 1992; Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-24059-4045/texto.

[3] República Argentina; Ley de Protección de los Datos Personales, Nro. 25326; sancionada el 4 de octubre de 2000, promulgada el 30 de octubre de 2000; Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-25326-49403/texto.

[4] República Argentina; Decreto Nº 727/06; Reglamentación de la Ley Nro. 23554; Recuperado de https://www.argentina.gob.ar/normativa/nacional/decreto-727-2006-119418/texto.

[5] Ministerio de Defensa (2020); Estrategia Nacional de Ciberdefensa; Buenos Aires: Ministerio de Defensa; Recuperado de https://www.argentina.gob.ar/defensa/ciberdefensa.

1.6. Ley de Telecomunicaciones (Nro. 19798): regula las comunicaciones en el ámbito nacional, incluyendo las comunicaciones de interés para la defensa y seguridad del país[6].

1.7. Resolución del Ministerio de Defesa N° 504/17 (Sistema de normalización de medios para la defensa): establece las características técnicas mínimas para sistemas de comunicación en el ámbito de defensa. Su enfoque principal es la interoperabilidad y seguridad en las comunicaciones tácticas, especialmente en entornos complejos y cambiantes[7].

2. Alcances y condiciones de la legislación nacional Argentina

De manera de articular las normativas descriptas con los alcances y condiciones sobre las actividades de comunicaciones, guerra electrónica y ciberdefensa se sintetiza en los siguientes aspectos:

2.1. Comunicaciones y guerra electrónica: las fuerzas armadas argentinas están habilitadas para utilizar sistemas de comunicaciones y realizar actividades de guerra electrónica bajo el marco de la Ley de Defensa Nacional Nro. 23554 y sus reglamentaciones. Esta ley define la defensa nacional como la acción coordinada de todas las fuerzas de la Nación para enfrentar agresiones de origen externo, y establece que las fuerzas armadas pueden emplearse disuasiva o efectivamente para este fin. La guerra electrónica, que históricamente se centraba en la tecnología analógica, ha evolucionado para incluir tácticas digitales y se complementa con las actividades de ciberdefensa.

2.2. Ciberdefensa: en Argentina está regulada y estructurada principalmente a través del Comando Conjunto de Ciberdefensa, creado en el año 2014. Este comando se encarga de la vigilancia y control de los sistemas cibernéticos militares, con el objetivo de identificar y neutralizar intrusiones y comportamientos anómalos en las redes militares. La formación y capacitación del personal en ciberdefensa se lleva a cabo en instituciones universitarias y en el Instituto de Ciberdefensa de las Fuerzas Armadas.

2.3. Marco legal y político: el decreto N° 727/2006 reglamenta la Ley de Defensa Nacional y establece que las fuerzas armadas pueden emplearse en situaciones de

[6] República Argentina; Ley de Telecomunicaciones, Nro. 19798; sancionada el 22 de agosto de 1972, promulgada el 23 de agosto de 1972; Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-19798-61479/texto.

[7] Ministerio de Defensa (2017); Resolución Ministerial Nº 504; Norma Def Com 1224; Comunicaciones: Redes tácticas de enlace de datos para el Comando y Control.

agresiones externas, pero no en asuntos de seguridad interior, que están regulados por la Ley de Seguridad Interior Nro. 24059. Además, la directiva de política de defensa nacional, actualizada en el año 2014, incorpora explícitamente la importancia del ciberespacio y la necesidad de adaptar los sistemas de defensa a estos nuevos componentes. La ciberdefensa es vista como una parte esencial de la defensa nacional y se enfoca en la legítima defensa contra agresiones militares de terceros estados.

2.4. Infraestructura crítica y ciberseguridad: el programa nacional de Infraestructura de Información Crítica y Ciberseguridad (ICIC), establecido por la resolución JGM N° 580/2011, tiene como objetivo definir y proteger la infraestructura estratégica y crítica del país. Este programa trabaja tanto con el sector público como con el privado para mejorar las capacidades de ciberseguridad en Argentina. La ley Nro. 26388[8], promulgada en 2008, modificó el código penal para incluir delitos cibernéticos, y la ley Nro. 26904[9] incorporó la figura del grooming.

3. Limitaciones de la legislación nacional Argentina

En Argentina, la realización de actividades de guerra electrónica y ciberoperaciones sin el establecimiento de un teatro de operaciones tiene limitaciones significativas. Estas restricciones están diseñadas para asegurar que las fuerzas armadas operen dentro de un marco legal específico y eviten interferir con la seguridad interior, que es jurisdicción de otras fuerzas y entidades del estado.

3.1. Limitaciones de la guerra electrónica

3.1.1. Ley de Defensa Nacional (Nro. 23554): define las condiciones y límites en los que las fuerzas armadas pueden actuar. Esta ley determina que las fuerzas armadas solo pueden ser utilizadas en el ámbito de la defensa nacional contra agresiones externas, y no para tareas de seguridad interior, excepto en situaciones excepcionales y bajo condiciones muy específicas.

[8] República Argentina; Ley Delitos Informáticos y Ciberseguridad; Nro. 26388; sancionada el 4 de junio de 2008, promulgada el 24 de junio de 2008; Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm.

[9] República Argentina; Ley Incorporación; Nro. 26904; sancionada el 13 de noviembre de 2013, promulgada el 4 de diciembre de 2013; Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm.

3.1.2. Las actividades de guerra electrónica están permitidas dentro del contexto de defensa nacional, pero no pueden ser desplegadas libremente sin la declaración formal de un teatro de operaciones que justifique su uso.

3.1.3. Reglamento de la Ley de Defensa Nacional (Decreto Nro. 727/2006): establece que cualquier operación de las fuerzas armadas debe ser en el contexto de un conflicto externo. La implementación de operaciones de guerra electrónica sin un teatro de operaciones predefinido y sin un conflicto declarado sería una violación de esta normativa.

3.2. Limitaciones de las ciberoperaciones

3.2.1. Comando Conjunto de Ciberdefensa[10]: tiene la responsabilidad de proteger los sistemas cibernéticos militares y responder a amenazas en el ciberespacio. Sin embargo, sus operaciones están limitadas a la defensa y protección de infraestructuras críticas y redes militares. La ejecución de ciberoperaciones ofensivas sin un mandato específico o fuera del contexto de defensa nacional y sin un teatro de operaciones definido sería ilegal.

3.2.2. Ley de Inteligencia Nacional (Nro. 25520)[11]: regula las actividades de inteligencia y contrainteligencia en Argentina, incluyendo ciberoperaciones. Las fuerzas armadas no pueden realizar actividades de inteligencia interna ni ciberoperaciones dentro del territorio nacional sin una justificación legal clara y sin el establecimiento de un teatro de operaciones específico. Cualquier actividad de ciberdefensa debe estar coordinada con las autoridades competentes y en el marco de la legalidad.

3.2.3. Programa Nacional de Infraestructura de Información Crítica y Ciberseguridad (ICIC): este programa establece un marco regulatorio para proteger infraestructuras críticas, pero no otorga autoridad para realizar ciberoperaciones ofensivas sin un mandato específico. Las actividades de

[10] Morales, Fernando; "Qué es y cómo funciona el Comando de Ciberdefensa, el equipo militar que actúa ante los ataques al sistema informático nacional"; Diario Infobae; Suplemento Política; Buenos Aires; 26 de marzo de 2022; Recuperado de https://www.infobae.com/politica/2022/03/26/que-es-y-como-funciona-el-comando-de-ciberdefensa-el-equipo-militar-que-actua-ante-los-ataques-al-sistema-informatico-nacional/

[11] República Argentina; Ley de Inteligencia Nacional; Nro. 25520; sancionada el 27 de noviembre de 2001, promulgada el 3 de diciembre de 2001; Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm.

ciberdefensa están enfocadas en la protección y respuesta a incidentes, no en la ofensiva sin un teatro de operaciones declarado[12].

4. Consideraciones adicionales de la legislación nacional Argentina

4.1. Separación de funciones entre defensa y seguridad interior: la Ley de Seguridad Interior (Nro. 24059) establece una clara separación de funciones entre las fuerzas armadas y las fuerzas de seguridad. Las fuerzas armadas no pueden intervenir en asuntos de seguridad interior sin una solicitud específica y bajo condiciones estrictas, lo que incluye la realización de operaciones electrónicas y cibernéticas.

4.2. Coordinación y autorización: cualquier operación de guerra electrónica o ciberoperación debe ser coordinada y autorizada por las autoridades competentes. Esto incluye la necesidad de aprobación por parte del Ministerio de Defensa y, en algunos casos, del Poder Ejecutivo Nacional. La falta de un teatro de operaciones formal implica que estas operaciones no pueden ser llevadas a cabo sin violar la normativa vigente.

5. Articulación de la legislación nacional vigente con la nueva estratégica de defensa nacional

5.1. Estrategia de defensa nacional

La legislación argentina sobre defensa se articula con la nueva estrategia de defensa nacional, que se basa en la integración y acción coordinada de todas las fuerzas de la nación para la resolución de conflictos que requieran el uso de las fuerzas armadas. Esta integración se lleva a cabo a través del Sistema de Defensa Nacional (SDN), que incluye al Presidente de la Nación, el Consejo de Defensa Nacional (CODENA), el Congreso de la Nación, el Ministerio de Defensa, el Estado Mayor Conjunto de las Fuerzas Armadas, el Ejército, la Armada, la Fuerza Aérea, la Gendarmería Nacional, la Prefectura Naval y el pueblo de la Nación.

La nueva estrategia de defensa nacional se basa en la concepción estratégica militar de restricción de área[13], que busca denegar el acceso del agresor al espacio propio y, en caso de que ingrese, negarle el control efectivo de áreas consideradas estratégicamente críticas. Esta concepción se implementa a través

[12] Revista Seguridad 360; "Estrategia de ciberseguridad en Argentina; Suplemento Noticias; 22 de Junio de 2022; Recuperado de https://revistaseguridad360.com/destacados/ciberseguridad-en-argentina-2/

[13] Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Doctrina Básica para la Acción Militar Conjunta – Proyecto;* PC 00-01; edición 2023; capítulo III; artículo 3.05; p. 31.

de cuatro capas de esfuerzos estratégicos: anticipar, prevenir, conjurar y repeler.

En la misma línea de la temática abordada se articula estrechamente con las limitaciones legales existentes para actividades de guerra electrónica y ciberdefensa en tiempos de paz y fuera de un teatro de operaciones formalmente establecido. Esta estrategia tiene como objetivo optimizar el uso del instrumento militar mediante una disuasión activa y la capacidad de operar en múltiples dominios, incluyendo el ciberespacio y la guerra electrónica.

La estrategia de restricción de área busca impedir o dificultar el acceso y la operación de fuerzas enemigas en áreas específicas, utilizando una combinación de sistemas defensivos y ofensivos avanzados. Esta estrategia incluye, por ejemplo, el desarrollo y despliegue de sistemas antiaéreos y misiles defensivos, que ofrecen capacidades significativas para la defensa aérea de mediano y corto alcance[14]. Otro ejemplo, el fortalecimiento de la capacidad de guerra electrónica y ciberdefensa a través de una nueva doctrina conjunta y la modernización de capacidades tecnológicas, se busca asegurar una respuesta eficaz en el dominio cibernético y en la guerra electrónica[15].

5.2. Limitaciones legales y operativas

En Argentina, las actividades de guerra electrónica y ciberdefensa están reguladas estrictamente por la legislación vigente. Según la Ley de Defensa Nacional (Nro. 23554), la acción militar en el ámbito de la defensa está restringida en tiempos de paz y se requiere la declaración de un teatro de operaciones para desplegar operaciones militares plenas, incluyendo aquellas en los dominios de guerra electrónica y ciberdefensa. Esto implica que:

5.2.1. Actividades limitadas en tiempo de paz: sin un conflicto declarado o una emergencia nacional, las fuerzas armadas no pueden llevar a cabo operaciones ofensivas en ciberespacio o guerra electrónica fuera de un contexto defensivo estricto o de entrenamiento.

5.2.2. Requerimiento de un teatro de operaciones: para desplegar plenamente las capacidades de guerra electrónica y ciberdefensa, es necesario establecer un

[14] Videla Solá, Mariano German; “Proyecto de Presupuesto 2024: Las Fuerzas Armadas Argentinas buscan incorporar sistemas de defensa antiaérea de mediano alcance”; Zona Militar; Recuperado de https://www.zona-militar.com/2023/09/20/presupuesto-2024-las-fuerzas-armadas-argentinas-buscan-incorporar-sistemas-de-defensa-antiaerea-de-mediano-alcance/

[15] Ministerio de Defensa; “Taiana participó de la presentación del ciclo de planeamiento de la Defensa Nacional”; Argentina.gob.ar; Recuperado de https://www.argentina.gob.ar/noticias/taiana-participo-de-la-presentacion-del-ciclo-de-planeamiento-de-la-defensa-nacional

teatro de operaciones. Esto asegura que cualquier acción esté legalmente respaldada y coordinada según los protocolos militares y legales establecidos.

6. Integración de la estrategia con las limitaciones legales

La estrategia de restricción de área se integra con estas limitaciones mediante un enfoque defensivo en tiempos de paz y la preparación para una rápida movilización y despliegue en caso de conflicto. Esto incluye:

6.3. Entrenamiento y preparación: continuar con ejercicios y simulaciones que preparen a las fuerzas armadas para una transición rápida a operaciones completas cuando sea necesario.

6.4. Modernización de capacidades: a través del Fondo Nacional de la Defensa (FONDEF), se busca recuperar y modernizar las capacidades críticas, asegurando que las fuerzas armadas estén equipadas con tecnología de vanguardia para operaciones en múltiples dominios.

7. La estrategia de restricción de área, las operaciones multidominio y la ventana de oportunidad

La estrategia de defensa nacional tiene una estrechan relación con las operaciones multidominio y su ejecución aprovechando las ventanas de oportunidad de las que podemos detallar:

7.1. La estrategia de restricción de área en Argentina está diseñada para impedir el acceso y operación de fuerzas enemigas en áreas estratégicas, y se relaciona estrechamente con el concepto de operaciones multidominio y el aprovechamiento de ventanas de oportunidad. Esta estrategia integra diversas capacidades en tierra, aire, mar, espacio y ciberespacio para lograr una defensa cohesionada y efectiva.

7.2. Operaciones multidominio: son aquellas que integran y sincronizan acciones en múltiples dominios de guerra (tierra, mar, aire, espacio y ciberespacio) para alcanzar objetivos estratégicos y tácticos. Este enfoque permite una mayor flexibilidad y capacidad de respuesta ante amenazas complejas y variadas.

7.3. Implementación en Argentina: la implementación de la estrategia de restricción de área y las operaciones multidominio en Argentina incluye:

7.3.1. Defensa integrada y coordinada: las fuerzas armadas argentinas buscan coordinar esfuerzos a través de diferentes dominios para maximizar la efectividad de la defensa nacional. Esto incluye la integración de capacidades

cibernéticas y electrónicas con las operaciones tradicionales de tierra, mar y aire.

7.3.2. Uso de tecnologías avanzadas: la modernización de las fuerzas armadas mediante el Fondo Nacional de la Defensa (FONDEF) es crucial para desarrollar capacidades avanzadas en guerra electrónica y ciberdefensa. Esto incluye la adquisición de nuevos sistemas antiaéreos, misiles defensivos, y tecnologías cibernéticas para reforzar la capacidad defensiva y ofensiva en todos los dominios.

7.4. Ventanas de Oportunidad: se refieren a momentos específicos en los que una fuerza puede explotar vulnerabilidades o ventajas temporales para lograr un objetivo militar. Estas ventanas pueden surgir debido a factores como el cambio en la situación táctica, la sorpresa, o la vulnerabilidad temporal del adversario.

7.5. Aprovechamiento en la estrategia Argentina

7.5.1. Guerra electrónica y ciberdefensa: en el dominio cibernético, las ventanas de oportunidad pueden incluir momentos en los que las redes del adversario están más vulnerables a ataques. La estrategia argentina busca desarrollar capacidades para identificar y explotar estas ventanas rápidamente, neutralizando amenazas antes de que puedan tener un impacto significativo.

7.5.2. Operaciones coordinadas: las operaciones multidominio permiten que las fuerzas armadas sincronicen acciones en diferentes dominios para maximizar el impacto. Por ejemplo, una operación de guerra electrónica que degrade las comunicaciones del adversario puede ser seguida por un ataque aéreo o terrestre coordinado para aprovechar la desorganización del enemigo.

7.5.3. Respuestas rápidas y flexibles: la capacidad de respuesta rápida es crucial para explotar ventanas de oportunidad. La estrategia de restricción de área implica estar preparado para desplegar rápidamente fuerzas y capacidades en cualquier dominio donde se identifique una ventaja temporal.

8. Conclusiones parciales

8.1. La legislación nacional argentina en relación con la defensa y seguridad, enfocada en actividades de comunicaciones, guerra electrónica y ciberdefensa, está cuidadosamente estructurada para abordar los desafíos contemporáneos en estos campos. El análisis de las normativas revela un marco legal sólido y adaptativo que facilita la defensa nacional, asegurando una operación eficiente y segura de las fuerzas armadas en tiempos de paz y conflicto.

8.2. La Ley de Defensa Nacional (Nro. 23554) proporciona los principios fundamentales que rigen la defensa nacional, incluyendo aspectos críticos de comunicaciones y guerra electrónica. Esta ley define la defensa nacional como la acción coordinada de todas las fuerzas de la nación para enfrentar agresiones de origen externo, habilitando el uso de sistemas de comunicaciones y tácticas de guerra electrónica. El Decreto N° 727/2006, que reglamenta esta ley, especifica las competencias y responsabilidades de las fuerzas armadas, garantizando que las actividades de defensa se realicen dentro de un marco regulado.

8.3. La Ley de Seguridad Interior (Nro. 24059) complementa la Ley de Defensa Nacional, enfocándose en la seguridad interior. Esta normativa es crucial para entender la delimitación de funciones entre las fuerzas armadas y las fuerzas de seguridad, asegurando que las operaciones de defensa no interfieran con asuntos de seguridad interior.

8.4. En el ámbito de la ciberdefensa, la Ley de Protección de los Datos Personales (Nro. 25326) es esencial porque regula el tratamiento de datos personales, estableciendo derechos y obligaciones que deben ser considerados en las operaciones de ciberdefensa. La protección de datos personales es fundamental para la seguridad nacional, ya que cualquier vulnerabilidad puede comprometer las infraestructuras críticas del país.

8.5. La Estrategia Nacional de ciberdefensa, aunque no es una ley, proporciona una visión integral y directrices específicas para la protección de infraestructuras críticas y la respuesta a amenazas cibernéticas. Esta estrategia, actualizada en 2020, destaca la importancia del ciberespacio en la defensa nacional y la necesidad de adaptar las capacidades de defensa a estos nuevos componentes.

8.6. La Ley de Telecomunicaciones (Nro. 19798) regula las comunicaciones en el ámbito nacional, incluyendo aquellas de interés para la defensa y seguridad del país. Esta ley es fundamental para asegurar que las comunicaciones estratégicas sean protegidas y eficientes.

8.7. En cuanto a los alcances y condiciones, la legislación establece claramente que las fuerzas armadas argentinas pueden utilizar sistemas de comunicaciones y realizar actividades de guerra electrónica bajo el marco de la Ley de Defensa Nacional y sus reglamentaciones. La evolución de la guerra electrónica, ahora integrada con tácticas digitales, complementa las actividades de ciberdefensa,

estructuradas principalmente a través del Comando Conjunto de Ciberdefensa, creado en 2014. Este comando se encarga de la vigilancia y control de los sistemas cibernéticos militares, con el objetivo de identificar y neutralizar intrusiones y comportamientos anómalos en las redes militares.

8.8. El marco legal y político se refuerza con el Programa Nacional de Infraestructura de Información Crítica y Ciberseguridad (ICIC), establecido por la Resolución JGM Nº 580/2011. Este programa trabaja tanto con el sector público como con el privado para mejorar las capacidades de ciberseguridad en Argentina. La legislación también aborda delitos cibernéticos mediante la Ley Nro. 26388 y la Ley Nro. 26904, que incorporan figuras legales relevantes como el grooming.

8.9. Finalmente, la implementación de la estrategia de restricción de área y operaciones multidominio, adoptada recientemente por Argentina, se articula estrechamente con las limitaciones legales existentes. Esta estrategia busca optimizar el uso del instrumento militar mediante una disuasión activa y la capacidad de operar en múltiples dominios, incluyendo el ciberespacio y la guerra electrónica. La modernización de capacidades tecnológicas y la preparación para una rápida movilización aseguran una respuesta eficaz a las amenazas, respetando siempre el marco legal vigente.

8.10. La legislación nacional argentina proporciona un marco firme y detallado que regula las actividades de comunicaciones, guerra electrónica y ciberdefensa, asegurando que estas operaciones se realicen de manera legal y coordinada, protegiendo así la seguridad nacional y los derechos de los ciudadanos.

Capítulo 2. Determinación de las características modulares en el ámbito militar de las comunicaciones, guerra electrónica y ciberdefensa

1. Modularidad: características en el ámbito de la ingeniería de sistemas y software

La modularidad en el contexto de la ingeniería de sistemas se define como la propiedad de un sistema que permite dividirlo en componentes o módulos independientes, cada uno de los cuales cumple una función específica y puede ser desarrollado, probado, modificado o reemplazado de forma aislada sin afectar al resto del sistema[16].

Un sistema complejo puede dividirse en piezas más simples llamadas módulos, un sistema compuesto de módulos es llamado modular. El principal beneficio de la modularidad es que permite la aplicación del principio de separación de intereses en dos fases: al enfrentar los detalles de cada módulo por separado ignorando detalles de los otros módulos, y al enfrentar las características globales de todos los módulos y sus relaciones para integrarlos en un único sistema coherente. Si estas fases son ejecutadas en ese orden se dice que el sistema es diseñado de abajo hacia arriba, en el orden inverso se dice que el sistema es diseñado de arriba hacia abajo. El principio de modularidad tiene tres objetivos principales: capacidad de descomponer un sistema complejo, capacidad de componerlo a partir de módulos existentes y comprensión del sistema en piezas o pedazos. La posibilidad de descomponer un sistema se basa en dividir en subproblemas de forma diseñada de arriba hacia abajo el problema original y luego aplicar el principio a cada subproblema en forma recursiva. Este procedimiento refleja el principio conocido de divide y vencerás. La posibilidad de componer un sistema está basada en obtener el sistema final de forma diseñada de abajo hacia arriba a partir de componentes elementales. Idealmente en la producción de software se quisiera poder ensamblar nuevas aplicaciones tomando módulos de una biblioteca y combinándolos para formar el producto requerido; estos módulos deberían ser diseñados con el objetivo expreso de ser reusables[17].

En la ingeniería de sistemas, un libro que profundiza en estas características

[16] Blanchard, B. S., Fabrycky, W. J.; Systems engineering and analysis; 5ta Edición; Pearson; Año 2013; p. 142.

[17] Carlo Ghezzi, Mehdi Jazayeri, Dino Mandrioli.; Fundamentals of Software Engineering; Prentice Hall; Edición 1991; capítulo 3; p. 49.

es “Ingeniería de Sistemas y Análisis” (en su versión original “Systems engineering and analysis”) de Benjamin S. Blanchard y Wolter J. Fabrycky. Este es una referencia clásica que aborda los conceptos fundamentales de la ingeniería de sistemas, incluyendo la importancia de la modularidad. A la cual se refiere a la división de un sistema en componentes o módulos que pueden ser independientes, modificados, reemplazables e intercambiables. Características fundamentales para la flexibilidad, escalabilidad, mantenibilidad, manejabilidad, adaptabilidad, facilidad para la prueba y depuración de sistemas, y verificable en forma independiente.

Un libro que aborda las características modulares con profundidad es “Ingeniería de Software” de Ian Sommerville. Obra que es considerada un texto fundamental en la disciplina de la ingeniería de software y ha sido ampliamente utilizada en la educación superior y en el ámbito profesional. Donde se puede mencionar que la modularidad es un principio de diseño que se aplica en la ingeniería de sistemas para crear estructuras complejas a partir de componentes más pequeños y manejables. Estas son algunas de las características clave de los sistemas modulares:

- Independencia funcional: cada módulo tiene funciones específicas, evitando la dependencia excesiva entre módulos. Esto permite un desarrollo y mantenimiento más eficaz de cada componente sin interferir con otros (Sommerville, 2011, p. 456).
- Cohesión: los elementos dentro de un módulo están interrelacionados para llevar a cabo su función. Esta cohesión contribuye a la organización interna de cada módulo, facilitando su comprensión y reutilización (Sommerville, 2011, p. 456).
- Acoplamiento bajo: los módulos están diseñados para minimizar sus conexiones y dependencias mutuas. Esto facilita su mantenimiento, actualización y escalabilidad (Sommerville, 2011, p. 456).
- Interfaz estándar: los módulos se comunican a través de interfaces definidas claramente, lo que permite la interoperabilidad entre ellos sin exponer detalles internos (Sommerville, 2011, p. 456).

- Reutilizable: los módulos están diseñados para ser utilizados en distintos sistemas o entornos, facilitando su implementación en proyectos futuros sin modificaciones significativas (Sommerville, 2011, p. 456).
- Combinable y ensamblable: los módulos pueden ser combinados o ensamblados para formar sistemas más complejos, conservando sus características individuales y funcionalidad independiente (Sommerville, 2011, p. 456).

Además de lo mencionado, pone un énfasis particular en los sistemas críticos, donde la modularidad es esencial para garantizar la seguridad y el rendimiento.

En la obra "Engineering Design: A Systematic Approach" de Pahl y Beitz, se refiere a las características modulares como a la utilización de componentes o unidades independientes que pueden combinarse y reorganizarse de diversas maneras para formar sistemas completos. Estas características incluyen:

- Intercambiabilidad: los módulos pueden ser reemplazados o actualizados sin afectar al resto del sistema.
- Flexibilidad: permite la adaptación y modificación del sistema mediante la adición, eliminación o reconfiguración de módulos.
- Escalabilidad: es posible ampliar el sistema mediante la incorporación de más módulos.
- Mantenimiento: la reparación y el mantenimiento son más fáciles y rápidos ya que solo se reemplazan o arreglan módulos específicos.
- Estandarización: los módulos siguen estándares predefinidos que aseguran compatibilidad y facilidad de integración.
- Eficiencia en producción y costos: la producción en masa de módulos estandarizados reduce costos y tiempo de fabricación.
- Mejora continua: permite la incorporación de nuevas tecnologías y mejoras sin necesidad de rediseñar todo el sistema.

A modo de finalizar el tópico, se concluye que la modularidad permite estructurar un sistema complejo en módulos o componentes independientes, cada uno cumpliendo funciones específicas y manejables. Las características principales de los sistemas modulares incluyen:

- La independencia funcional de cada módulo, permitiendo su desarrollo y mantenimiento sin afectar a otros.
- Una cohesión interna en cada módulo que asegura que todos sus elementos están alineados para cumplir su función.
- Un bajo acoplamiento entre módulos, minimizando las interdependencias.
- El uso de interfaces estándar facilita la comunicación y colaboración entre módulos, aumentando la interoperabilidad.
- Módulos reutilizables, diseñados para adaptarse a diferentes sistemas y entornos sin mayores cambios, lo que incrementa la eficiencia en el desarrollo y los costos de producción.
- Módulos combinables en diversas configuraciones, lo que permite un sistema escalable y adaptable a cambios tecnológicos sin necesidad de rediseñarlo completamente.

2. Modularidad: análisis de publicaciones y artículos militares

La modularidad en los sistemas militares es un enfoque clave que ha ganado relevancia en las últimas décadas, especialmente en el contexto de las operaciones conjuntas y multinacionales lideradas por organizaciones como la OTAN y el departamento de defensa de los Estados Unidos. A continuación, se bosquejará un análisis detallado basado en las publicaciones y estudios de casos disponibles:

2.1. Definición y concepto de modularidad: se refiere a la capacidad de un sistema para ser dividido en módulos o componentes intercambiables y autónomos que pueden ser fácilmente reemplazados, actualizados o reconfigurados para cumplir con diferentes misiones o escenarios operacionales. Este enfoque permite una mayor flexibilidad, adaptabilidad y sostenibilidad en entornos de combate dinámicos.

2.2. Ventajas de la modularidad en sistemas militares

2.2.1. Flexibilidad operacional: la modularidad permite a las fuerzas armadas adaptar rápidamente sus capacidades a diferentes escenarios de misión sin necesidad de desarrollar y desplegar sistemas completamente nuevos. Por ejemplo, un vehículo militar modular puede ser equipado con diferentes paquetes de sensores, armamento o sistemas de comunicación según las necesidades del campo de batalla.

2.2.2. Mantenimiento y sostenibilidad: los sistemas modulares facilitan el mantenimiento y la reparación, ya que los módulos dañados pueden ser reemplazados rápidamente en lugar de reparar o reemplazar sistemas completos. Esto reduce los tiempos de inactividad y aumenta la disponibilidad operativa.

2.2.3. Escalabilidad: los sistemas modulares pueden ser escalados en función de la amenaza o el entorno operativo. Por ejemplo, una fuerza puede desplegar una configuración mínima en un escenario de baja amenaza y aumentar la complejidad del sistema si la situación lo requiere.

2.2.4. Interoperabilidad multinacional: en operaciones conjuntas, especialmente dentro de la OTAN, la modularidad facilita la interoperabilidad entre las fuerzas de diferentes naciones, permitiendo que los sistemas de diferentes países trabajen juntos de manera eficiente. Algo que no sucede en el mismo orden en las fuerzas armadas argentinas, donde la interoperabilidad permite lograr la modularidad[18].

2.3. Aplicaciones prácticas de la modularidad en el contexto militar: aunque los ejemplos mencionados equivalen al nivel táctico, debemos centrarnos en que las operaciones multidominio son operaciones tácticas conducidas por un Comandante Operacional.

2.3.1. Vehículos terrestres: un ejemplo destacado es el programa de Vehículos de Combate Blindados Modulares (Modular Armored Vehicles, MAV) del Departamento de Defensa de los Estados Unidos, donde se desarrollan vehículos que pueden ser configurados para misiones específicas como reconocimiento, transporte de tropas o apoyo de fuego, cambiando módulos como el armamento o la protección balística.

2.3.2. Sistemas de defensa aérea y naval: la modularidad también se aplica en sistemas de defensa aérea y naval, donde las plataformas pueden ser equipadas con diferentes módulos de sensores, sistemas de armas o contramedidas electrónicas para responder a amenazas aéreas, submarinas o de superficie.

2.3.3. Tecnología de la información y comunicaciones (TIC): los sistemas modulares son esenciales en la arquitectura de redes militares, permitiendo la integración

[18] Ejército Argentino; *Conducción de las Fuerzas Terrestres;* ROB 00-01; edición 2015*;* capitulo II; artículo 2025 y 2026; p. 39.

de nuevas tecnologías y la interoperabilidad entre sistemas de comunicación de diferentes ramas o países.

2.4. Desafíos de la implementación de sistemas modulares

2.4.1. Complejidad de integración: a pesar de sus ventajas, la integración de sistemas modulares puede ser compleja y requerir estándares y protocolos estrictos para garantizar que los módulos de diferentes fabricantes o países puedan operar juntos sin problemas.

2.4.2. Costo inicial y desarrollo: el desarrollo de sistemas modulares puede ser costoso inicialmente, ya que requiere una planificación detallada y pruebas exhaustivas para garantizar la compatibilidad y la funcionalidad.

2.4.3. Seguridad y ciberseguridad: los sistemas modulares pueden ser más vulnerables a ataques cibernéticos si no se implementan adecuadas medidas de seguridad en cada módulo. Además, la interconexión de múltiples módulos aumenta la superficie de ataque potencial.

2.5. Estudios de caso y publicaciones relevantes

2.5.1. Estudio de la OTAN sobre vehículos de combate modulares: este estudio destaca cómo la OTAN ha implementado vehículos modulares en misiones en Europa del Este, permitiendo una respuesta rápida y adaptada a las amenazas cambiantes en la región.

2.5.2. Informe del DTIC[19] sobre sistemas modulares de defensa aérea: Este informe analiza la efectividad de los sistemas modulares en la defensa aérea, especialmente en la integración de sensores y sistemas de armas de diferentes naciones para crear una red de defensa cohesiva.

2.5.3. Caso del sistema de gestión de combate modular (MCS) del DoD[20]: Este sistema ha permitido al cuerpo de marina de los Estados Unidos mejorar la capacidad de sus buques para adaptarse rápidamente a diferentes misiones mediante la incorporación de módulos de sensores y armas según la necesidad.

2.5.4. La información proveniente de las revistas especializadas Jane's Defence Weekly y Military & Aerospace Electronics con respecto a la modularidad en sistemas militares:

2.5.4.1. Modularidad en tecnología de defensa según Jane’s Defence Weekly[21]

[19] Defense Technical Information Center.
[20] Departamento de Defensa de los Estados Unidos de Norteamérica (DoD).
[21] Jane's Defence Weekly; *Analysis of Modular Systems in Modern Military Programs;* Jane's

2.5.4.1.1. Tendencias en sistemas modulares: ésta revista es una fuente clave para analizar las tendencias actuales en tecnología de defensa, y uno de sus focos recientes ha sido la evolución de sistemas modulares en diversas áreas militares. Los artículos destacan cómo la modularidad está redefiniendo las capacidades de las fuerzas armadas al permitir una rápida adaptación a amenazas emergentes.

2.5.4.1.2. Programas de defensa modernos: la revista ha cubierto extensivamente programas como el Future Combat Systems (FCS), que se basa en la modularidad para ofrecer una mayor flexibilidad en operaciones conjuntas. Estos programas están diseñados para facilitar la interoperabilidad entre diferentes ramas de las fuerzas armadas y, en algunos casos, entre fuerzas multinacionales.

2.5.4.1.3. Desarrollo y actualización de plataformas: aborda cómo las plataformas militares modulares permiten una actualización continua, asegurando que las fuerzas armadas puedan mantener sus sistemas al día con las últimas tecnologías sin necesidad de reemplazar completamente sus equipos.

2.5.4.2. Modularidad en Tecnología Electrónica y Militar según Military & Aerospace Electronics[22]

2.5.4.2.1. Enfoque en la electrónica modular: se centra en cómo la modularidad se ha convertido en un componente esencial de la electrónica militar. La modularidad en los sistemas electrónicos no solo facilita la integración de nuevas tecnologías, sino que también mejora la sostenibilidad y la eficiencia operativa.

2.5.4.2.2. Sistemas de mando y control (C2): los artículos en Military & Aerospace Electronics a menudo cubren la importancia de la modularidad en sistemas de mando y control, donde los módulos electrónicos pueden ser fácilmente reemplazados o actualizados para mejorar la capacidad de respuesta ante diferentes escenarios operativos. Por ejemplo, la integración de módulos para mejorar la ciberseguridad o la comunicación en tiempo real.

Information Group; s.f.; recuperado de https://www.janes.com

[22] Military & Aerospace Electronics; *Modular Electronics and Their Impact on Military Communication and Radar Systems*; Military & Aerospace Electronics; s.f.; recuperado de https://www.militaryaerospace.com

2.5.4.2.3. Tecnología de radar y sensores: la revista también ha destacado cómo la modularidad está siendo aplicada en tecnologías de radar y sensores, permitiendo que estos sistemas sean adaptables a diferentes plataformas y entornos. Esto es especialmente relevante en el desarrollo de sistemas de detección para vehículos aéreos no tripulados (UAVs) y sistemas de defensa antiaérea.

2.5.4.3. Desafíos y consideraciones según las revistas

2.5.4.3.1. Interoperabilidad y compatibilidad: Un tema recurrente en ambas publicaciones es el desafío de garantizar la interoperabilidad y compatibilidad de los módulos en diferentes plataformas y entre distintas naciones. Jane's Defence Weekly, en particular, ha señalado que la falta de estándares internacionales puede dificultar la integración efectiva de sistemas modulares en operaciones conjuntas.

2.5.4.3.2. Ciberseguridad en sistemas modulares: Military & Aerospace Electronics ha destacado los riesgos cibernéticos asociados con la modularidad, señalando que cada módulo adicional puede introducir nuevas vulnerabilidades. La necesidad de desarrollar módulos con ciberseguridad integrada es un tema clave en sus análisis.

3. Modularidad: determinación de las características para las comunicaciones, guerra electrónica y ciberdefensa

La modularidad en los sistemas militares no solo tiene un impacto profundo en las plataformas físicas como vehículos y buques, sino que también juega un papel crucial en los ámbitos de las comunicaciones, la guerra electrónica y la ciberdefensa. A continuación, se presenta un análisis de cómo se relaciona la modularidad con estas áreas principales para el comando y control:

3.1. La modularidad en las comunicaciones

Las características modulares que deben tener las comunicaciones a nivel operacional son fundamentales para garantizar la eficiencia y adaptabilidad en los entornos operativos modernos. A continuación, se presenta una articulación de estas características con la doctrina especifica del Ejército Argentino, del Estado Mayor Conjunto y publicaciones militares de fuentes abiertas, particularmente de Estados Unidos y Gran Bretaña sobre la temática:

3.1.1. Independencia funcional: cada módulo del sistema de comunicación debe ser autónomo y cumplir funciones específicas, lo que permite su integración,

actualización o reemplazo sin afectar al sistema completo. Este enfoque modular facilita la configuración dinámica en entornos de combate. Por ejemplo los sistemas de radio definido por software (SDR) del Ejército de los Estados Unidos permiten la reconfiguración rápida de las señales para adaptarse a distintos tipos de misión. Estos módulos independientes aseguran la continuidad de las operaciones a pesar de cambios en el entorno[23].

3.1.2. Interoperabilidad: como lo menciona la doctrina específica del Ejército Argentino; es la característica que se debe cumplir para lograr la modularidad[24]. La interoperabilidad permite que los sistemas modulares de comunicación sean compatibles con diferentes plataformas y tecnologías, esencial para operaciones conjuntas entre distintos servicios o naciones. Esto se logra a través de estándares abiertos y protocolos comunes, como en el enfoque MOSA (Modular Open Systems Approach), que facilita la integración de sistemas C5ISR[25] en múltiples dominios. Por ejemplo en el Reino Unido, la Generic Vehicle Architecture (GVA) estandariza los módulos para vehículos terrestres, garantizando que los sistemas de comunicación se integren eficazmente en diversas plataformas y escenarios[26].

3.1.3. Escalabilidad: los sistemas de comunicaciones deben ser escalables para adaptarse a las necesidades operacionales cambiantes. Esto implica que los módulos se puedan agregar o quitar según la magnitud de la misión o el área de cobertura necesaria, permitiendo una respuesta flexible. Por ejemplo las radios multibanda de las fuerzas armadas brasileñas permiten la escalabilidad mediante la adición de módulos para operar en diversas frecuencias, lo que es crucial en escenarios con limitaciones de infraestructura[27].

3.1.4. Reutilización de componentes: la modularidad permite la reutilización de módulos en diferentes configuraciones o sistemas, optimizando los recursos y reduciendo costos. Los módulos reutilizables garantizan que los equipos sean

---

[23] Curtiss-Wright; *MOSA (Modular Open Systems Approach) for military systems;* Año 2024; p. 6; recuperado de https://www.curtisswrightds.com

[24] Ejército Argentino; *Conducción de las Fuerzas Terrestres;* ROB 00-01; edición 2015*;* capitulo II; artículo 2025 y 2026; p. 39.

[25] Command (Comando), C – Control; C - Communications (Comunicaciones); C - Computers (Computadoras); I - Intelligence (Inteligencia); S - Surveillance (Vigilancia); R - Reconnaissance (Reconocimiento).

[26] Army Technology; *The evolution of military comms: From radios to advanced digital systems;* Año 2023; pp. 15-17; recuperado de https://www.army-technology.com

[27] Modern Battlespace; *The demand for military interoperability is resulting in modular comms approaches;* Año 2018; p. 23; recuperado de https://www.modernbattlespace.com

compatibles en diversos entornos operacionales sin necesidad de rediseños extensivos. Por ejemplo las radios DMR (Digital Modular Radio) de los Estados Unidos son reutilizables en múltiples plataformas, lo que reduce la necesidad de adquirir diferentes sistemas para cada tipo de operación[28].

3.1.5. Automatización y respuesta rápida: los sistemas de comunicaciones deben incluir capacidades de automatización para mejorar la eficiencia operativa y la velocidad de respuesta. La automatización permite la detección rápida de problemas o interferencias y la reconfiguración automática del sistema para mantener la comunicación segura. Por ejemplo los sistemas C5ISR de los Estados Unidos utilizan módulos automatizados que identifican automáticamente interferencias en el espectro y cambian a canales seguros para asegurar la comunicación continua[29].

3.1.6. Integración en tiempo real: los módulos deben ser capaces de compartir información en tiempo real, lo cual es crucial para operaciones multidominios. La integración en tiempo real garantiza que los datos recopilados por diferentes sensores y plataformas se utilicen de manera efectiva para la toma de decisiones conjuntas operativas. Por ejemplo el Sensor Open Systems Architecture (SOSA) en los Estados Unidos facilita la integración en tiempo real de datos provenientes de diferentes sensores y sistemas de comunicación, permitiendo una rápida coordinación en el campo de batalla[30].

3.2. La modularidad en la guerra electrónica

Se analizará en forma independiente, pero en la actualidad actúa en forma articulada y vinculada con la ciberdefensa. Para armonizar las características modulares de la guerra electrónica con los principios de ingeniería de software expuestos por Ian Sommerville, es esencial comprender cómo los sistemas de software modularizados, descritos en el contexto de la guerra electrónica, se alinean con los enfoques de desarrollo modular, confiabilidad y seguridad que Sommerville propone.

3.2.1. Interoperabilidad y escalabilidad: Sommerville destaca la importancia de la

[28] Curtiss-Wright; *MOSA (Modular Open Systems Approach) for military systems;* Año 2024; p. 8; recuperado de https://www.curtisswrightds.com

[29] Army Technology; *The evolution of military comms: From radios to advanced digital systems*; Año 2023; p. 22; recuperado de https://www.army-technology.com

[30] Curtiss-Wright; *MOSA (Modular Open Systems Approach) for military systems;* Año 2024; pp. 10-12; recuperado de https://www.curtisswrightds.com

interoperabilidad y escalabilidad en los sistemas de software distribuidos. Estos principios son esenciales en el diseño de sistemas de guerra electrónica donde los módulos deben poder interoperar con plataformas aéreas, terrestres y marítimas de diferentes aliados. También subraya la capacidad de escalar un sistema según las necesidades de la organización, lo cual es un principio central en la guerra electrónica, donde los módulos pueden adaptarse a misiones tácticas, operacionales o estratégicas. Por ejemplo los sistemas modulares de guerra electrónica de Rusia, como el Krasukha-4, permiten ajustar la escala de las operaciones de interferencia según la magnitud del conflicto, integrando capacidades de ataque electrónico con sistemas de defensa aérea[31].

3.2.2. Reutilización y flexibilidad: en ingeniería de software, la reutilización de módulos permite la creación de sistemas más eficientes y con menor costo. Sommerville explica que la flexibilidad es esencial para que los componentes de software puedan ser reutilizados en diferentes contextos. Esta flexibilidad también se traduce en la guerra electrónica, donde los módulos de apoyo electrónico pueden configurarse para diferentes misiones de inteligencia o ataque. Por ejemplo los sistemas de apoyo electrónico de España reutilizan módulos SIGINT[32] para recopilar información de señales en diversos escenarios, adaptándose a las necesidades de cada misión[33].

3.2.3. Automatización y respuesta autónoma: Sommerville argumenta que la automatización es clave para mejorar la eficiencia en los sistemas de software, un principio que se aplica también a los sistemas de guerra electrónica. En este contexto, los módulos automatizados pueden tomar decisiones rápidas sin intervención humana, lo que es esencial en escenarios de respuesta rápida. Dando lugar al creciente empleo de la Inteligencia Artificial (IA) para esta característica. Por ejemplo los sistemas de guerra electrónica de los Estados Unidos, como el AN/ALQ-218, incluyen módulos automatizados que responden rápidamente a amenazas de misiles guiados por radar, activando

[31] Nieto, Ignacio; *¿Por qué lo llamas ciber cuando quieres decir guerra electrónica?*; *Global Strategy Report* 9/2023; Año 2023; recuperado de https://global-strategy.org/por-que-lo-llamas-ciber-cuando-quieres-decir-guerra-electronica/.

[32] SIGINT: Signal Intelligence – Inteligencia de Señales.

[33] Álvarez, Salvador; *Guerra electrónica: el campo de batalla silencioso del futuro*; Grupo Oesía; Año 2023; recuperado de https://grupooesia.com/insight/guerra-electronica-el-campo-de-batalla-silencioso-del-futuro/.

contramedidas de manera autónoma[34].

3.2.4. Integración en tiempo real: es una característica fundamental de los sistemas de software modernos según Sommerville, ya que permite que diferentes componentes del sistema trabajen juntos sin necesidad de detener o reiniciar el sistema. Este principio es crucial en la guerra electrónica, donde los módulos deben integrarse y compartir datos en tiempo real para garantizar una respuesta coordinada y eficaz a las amenazas. Por ejemplo en las operaciones conjuntas de la OTAN, los módulos de guerra electrónica comparten datos de inteligencia en tiempo real, lo que permite una respuesta rápida y efectiva a las amenazas emergentes en múltiples dominios[35].

3.3. La modularidad en la ciberdefensa (CD)

A continuación, se detalla las características que hacen que un sistema de ciberdefensa sea modular:

3.3.1. Arquitectura en módulos independientes[36]: los sistemas deberían poder ser integrados, actualizados o reemplazados sin afectar a todo el sistema. Por ejemplo cada subsistema puede corresponder a un componente específico, como la gestión de incidentes, la autenticación de usuarios o la detección de intrusos. Estos operan de forma autónoma, pero pueden comunicarse entre sí cuando es necesario. Permite la escalabilidad y la actualización progresiva de las capacidades de ciberdefensa sin detener todo el sistema.

3.3.2. Integrabilidad[37]: los sistemas deberían poder integrarse fácilmente con otros sistemas o infraestructuras de defensa cibernética, tanto a nivel nacional como internacional. Por ejemplo los sistemas pueden estar diseñados para compartir datos e información sobre amenazas con otros sistemas, como los utilizados por los aliados en la OTAN o agencias gubernamentales. Esto mejora la colaboración y la efectividad de las operaciones de ciberdefensa conjuntas.

[34] Bueno, Francisco José Matías; *Electronic Warfare*; Revista Ejércitos; Año 2019; recuperado de https://www.revistaejercitos.com/en/articulos/la-guerra-electronica-la-gran-ventaja-rusa/.

[35] Nieto, Ignacio; *¿Por qué lo llamas ciber cuando quieres decir guerra electrónica?*; *Global Strategy Report* 9/2023; Año 2023; recuperado de https://global-strategy.org/por-que-lo-llamas-ciber-cuando-quieres-decir-guerra-electronica/.

[36] Moyano, T. R.; *La República Argentina y sus esfuerzos en ciberdefensa*; Visión Conjunta Nro 22; Año 2020, p. 53.

[37] Cañete, P. A.; *El comando de ciberdefensa alemán: un claro ejemplo de integración*; Visión Conjunta Nro 22; Año 2020; p. 56.

3.3.3. Escalabilidad[38]: un sistema de CD debería poder adaptarse a las necesidades crecientes o decrecientes de la organización, permitiendo la incorporación o eliminación de módulos según la demanda. Por ejemplo durante un ataque de denegación de servicio (DDoS), se pueden añadir módulos de mitigación adicionales para gestionar el tráfico de manera más eficiente. Ello facilita la adaptación a situaciones cambiantes sin la necesidad de rediseñar o detener el sistema completo.

3.3.4. Flexibilidad en la respuesta a amenazas[39]: cada sistema tiene una función específica y puede ser reconfigurado o ajustado para responder a diferentes tipos de amenazas o ataques cibernéticos. Por ejemplo un sistema de análisis de malware puede ser actualizado para detectar nuevas variantes de malware o adaptarse para operar en diferentes plataformas. El beneficio es garantizar una respuesta rápida y eficiente ante una amplia gama de amenazas, desde ataques de phishing hasta intrusiones complejas.

3.3.5. Autonomía operativa[40]: los sistemas de CD deberían operar de manera autónoma y no dependen completamente unos de otros, lo que permite que cada uno funcione independientemente o en conjunto. Por ejemplo un sistema de defensa perimetral puede funcionar independientemente del sistema de monitorización interna de la red, pero ambos pueden interactuar si es necesario. Cuyo beneficio será evitar que una falla en un módulo afecte a todo el sistema, aumentando la resiliencia global.

3.3.6. Capacidad de actualización[41]: los sistemas de CD se pueden actualizar de manera independiente sin necesidad de reemplazar o interrumpir el funcionamiento del sistema completo. Por ejemplo un sistema de firewall puede ser actualizado con nuevas reglas de filtrado sin afectar a los módulos de detección de intrusiones o de respuesta a incidentes. El beneficio principal será minimizar el tiempo de inactividad y permite una evolución continua de las capacidades de defensa frente a nuevas amenazas.

---

[38] Moresi, A. A.; *El conflicto futuro*; Visión Conjunta Nro 22; Año 2020; p. 60.

[39] Cundins, E.; *El factor militar como medio de prevención pacífica de conflictos*; Visión Conjunta Nro 22; Año 2020; p. 62.

[40] Cañete, P. A.; *El comando de ciberdefensa alemán: un claro ejemplo de integración*; Visión Conjunta Nro 22; Año 2020; p. 63.

[41] Moyano, T. R.; *La República Argentina y sus esfuerzos en ciberdefensa*; Visión Conjunta Nro 22; Año 2020, p. 64.

3.3.7. Reutilizable[42]: los sistemas de ciberdefensa pueden ser reutilizados o adaptados para diferentes escenarios y plataformas sin necesidad de diseñar soluciones desde cero. Por ejemplo un módulo de cifrado puede ser implementado en múltiples capas de seguridad, como en la protección de datos de comunicación y en el almacenamiento de información. Se puede mencionar los beneficio de que reduce los costos y el tiempo de desarrollo, maximizando la eficiencia operativa.

3.3.8. Automatización: es clave en sistemas modulares, permitiendo que los módulos realicen tareas repetitivas o respuestas automáticas a incidentes sin intervención humana constante. Por ejemplo un módulo de detección de anomalías puede activar automáticamente un módulo de respuesta, que aísla una sección de la red cuando detecta un comportamiento anómalo. Esto mejora los tiempos de respuesta y permite la operación continua frente a amenazas complejas o voluminosas.

3.3.9. Integración en tiempo real: los módulos pueden integrarse en tiempo real, ajustándose a los cambios en la infraestructura de ciberseguridad sin necesidad de interrumpir las operaciones. Por ejemplo durante un ataque, un módulo de análisis forense puede comenzar a interactuar con el módulo de inteligencia cibernética para identificar patrones y compartir datos relevantes sobre la amenaza en curso. Ello aumenta la agilidad del sistema para adaptarse a situaciones de crisis sin demoras.

[42] Moresi, A. A.; *El conflicto futuro*; Visión Conjunta Nro 22; Año 2020; p. 65.

Conclusiones

Esta investigación trata sobre las características del criterio de modularidad en el diseño de un elemento de comunicaciones, guerra electrónica y ciberdefensa, así el objetivo que se plantea es analizar las características modulares que debería reunir ese elemento para favorecer la conducción de un comandante en operaciones multidominio. De ello se desprenden dos objetivos específicos, el primero analizar las actividades de comunicaciones, guerra electrónica y ciberdefensa a desarrollar en las operaciones multidominio a la luz de la legislación argentina vigente. Y el segundo identificar las características modulares para conformar un elemento de comunicaciones, guerra electrónica y ciberdefensa

Relacionado con el primer objetivo específico, las actividades de comunicaciones, guerra electrónica y ciberdefensa en las operaciones multidominio representan un enfoque integral en el que se combinan y sincronizan las capacidades en los dominios terrestre, aéreo, marítimo, espacial y cibernético para lograr superioridad operacional. En el contexto argentino, es esencial que las actividades de comunicaciones, guerra electrónica y ciberdefensa se desarrollen conforme a la legislación nacional, garantizando el respeto a la soberanía y a los derechos establecidos.

La Ley de Defensa Nacional (Ley Nro. 23554) y la Ley de Seguridad Interior (Ley Nro. 24059) proporcionan el marco legal para las acciones de las fuerzas armadas y de seguridad en Argentina. Estas leyes establecen que las fuerzas armadas tienen como misión principal la defensa de la integridad territorial y la soberanía nacional. Bajo este marco, las actividades de comunicaciones, guerra electrónica y ciberdefensa deben orientarse a:

a. Comunicaciones Seguras y Resilientes: implementar sistemas de comunicaciones que aseguren la confidencialidad, integridad y disponibilidad de la información. Esto implica el uso de cifrado robusto, autenticación multifactor y protocolos seguros, en cumplimiento con las normativas de protección de datos y seguridad de la información.
b. Guerra Electrónica: desarrollar capacidades para detectar, identificar y neutralizar las amenazas en el espectro electromagnético. Esto incluye acciones de inteligencia electrónica, interferencia y protección electrónica, siempre respetando las regulaciones nacionales sobre el uso del espectro radioeléctrico y evitando afectar a las comunicaciones civiles.

c. Ciberdefensa: fortalecer la protección de infraestructuras críticas y sistemas de información ante ciberataques. La creación de equipos especializados en respuesta a incidentes cibernéticos y la colaboración con organismos nacionales como el Equipo de Respuesta ante Emergencias Informáticas de la República Argentina (ArCERT) son fundamentales. Estas acciones deben alinearse con la Estrategia Nacional de Ciberseguridad y las normativas internacionales suscritas por el país.

Además, es necesario considerar:

a. Capacitación y formación: impulsar programas de formación y adiestramiento para el personal en áreas de ciberdefensa, guerra electrónica y comunicaciones avanzadas, garantizando que estén actualizados frente a las últimas amenazas y tecnologías.
b. Colaboración interagencial: fomentar la cooperación entre las diferentes ramas de las fuerzas armadas, fuerzas de seguridad y organismos civiles para lograr una respuesta coordinada y efectiva en operaciones multidominio por las limitaciones y restricciones que se le presentan a estas actividades ante las nuevas amenazas consideradas híbridas.
c. Desarrollo tecnológico nacional: promover la investigación y el desarrollo de tecnologías autóctonas que reduzcan la dependencia de sistemas extranjeros, potenciando la industria nacional de defensa y asegurando la soberanía tecnológica.

Las actividades mencionadas deben llevarse a cabo respetando los derechos humanos y las libertades individuales, tal como establece la Constitución Nacional y los tratados internacionales ratificados por Argentina.

Con respecto al segundo objetivo específico, luego del desarrollo del presente trabajo se determinaron las consecuentes características de la modularidad en los sistemas de comunicaciones, guerra electrónica y ciberdefensa. Ellas permiten diseñar sistemas flexibles, escalables y adaptables, optimizando recursos y mejorando la capacidad de respuesta. Para conformar un elemento efectivo en comunicaciones, guerra electrónica y ciberdefensa, se identifican las siguientes características modulares:

a. Flexibilidad: los módulos, del elemento que se quiera conformar, deben ser fácilmente configurables y reconfigurables, permitiendo adaptarse rápidamente a diferentes escenarios y misiones. Esto es vital en entornos dinámicos donde las amenazas y necesidades pueden cambiar de forma abrupta.

b. Interoperabilidad: los módulos deben cumplir con estándares internacionales y nacionales que aseguren su compatibilidad con sistemas de otras unidades y fuerzas en el ámbito conjunto y combinado. Esto facilita las operaciones conjuntas y multinacionales, permitiendo una integración fluida de capacidades.
c. Escalabilidad: los sistemas modulares deben permitir la ampliación o reducción de capacidades según las necesidades operativas y los escenarios donde se deberá cumplir la misión. Por ejemplo, agregar módulos de procesamiento adicional en ciberdefensa o ampliar el alcance y redundancia en comunicaciones.
d. Mantenibilidad y Sostenibilidad: la modularidad simplifica el mantenimiento al permitir la sustitución rápida de módulos defectuosos sin afectar al sistema completo. Esto reduce tiempos de inactividad y facilita la logística de repuestos y actualizaciones.
e. Actualización Tecnológica: los módulos deben diseñarse para facilitar la incorporación de nuevas tecnologías y mejoras, a lo que muchas industrias de la defensa llaman "pods"[43]. Esto es crucial para mantener la superioridad tecnológica frente a adversarios y adaptarse a nuevas amenazas.
f. Estándares de Seguridad: cada módulo debe integrar medidas de seguridad cibernética y protección electrónica para prevenir vulnerabilidades. La seguridad debe considerarse desde el diseño, incorporando principios de "seguridad por defecto".
g. Interfaces Estándar: el uso de interfaces y protocolos estándar permite la comunicación efectiva entre módulos y sistemas, facilitando la integración y reduciendo la complejidad en la interoperabilidad.
h. Reutilización y Combinación: los módulos deben ser reutilizables en diferentes sistemas y contextos, permitiendo combinaciones diversas para cumplir con requerimientos específicos. Esto maximiza la eficiencia y reduce costos de desarrollo.

En el ámbito argentino, la adopción de estas características modulares implica:

[43] Los "pods" son módulos o contenedores externos que se pueden acoplar a aeronaves, vehículos o plataformas militares para proporcionar capacidades adicionales sin requerir modificaciones permanentes en el sistema principal. Estos pods están diseñados para ser aerodinámicos y pueden ser intercambiados según las necesidades de la misión.

a. Desarrollo de normativas y estándares nacionales: establecer lineamientos claros que definan las especificaciones técnicas y estándares a utilizar en los módulos, promoviendo la uniformidad y compatibilidad entre sistemas.
b. Inversión en Investigación y Desarrollo (I+D): fomentar proyectos de I+D que impulsen la creación de tecnologías modulares nacionales, involucrando a universidades, centros de investigación y la industria para la defensa.
c. Colaboración público-privada: establecer alianzas y convenios con empresas nacionales e internacionales que aporten experiencia y tecnologías avanzadas, asegurando transferencia de conocimiento y desarrollo local.
d. Formación especializada: implementar programas de capacitación para el personal militar y civil en diseño, implementación y mantenimiento de sistemas modulares, asegurando el capital humano necesario para su operación efectiva. Aunque exista profesionales dentro del ámbito militar, generar estímulos e incentivos para no perder el capital que se forma y se posee.
e. Políticas de adquisición estratégica: priorizar la adquisición de sistemas y tecnologías que cumplan con los principios de modularidad, garantizando así la coherencia en las capacidades operativas y facilitando futuras actualizaciones.

La implementación de sistemas modulares en comunicaciones, guerra electrónica y ciberdefensa permitirá a las Fuerzas Armadas Argentinas contar con herramientas versátiles y adaptables, esenciales para el éxito en operaciones multidominio en la actualidad. Esto no solo mejora la eficiencia operativa sino que también contribuye a la optimización de recursos y al fortalecimiento de la industria nacional de defensa.

Bibliografía

Álvarez, Salvador (2023); *Guerra electrónica: el campo de batalla silencioso del futuro*; Grupo Oesía; Recuperado de https://grupooesia.com/insight/guerra-electronica-el-campo-de-batalla-silencioso-del-futuro/.

Anca, L. (2015); *"La ciberdefensa: hacia el desarrollo de una interoperabilidad conjunta del teatro de operaciones";* Trabajo Final Integrador de Especialización; Escuela Superior de Guerra Conjunta; Buenos Aires.

Armada Argentina; *Publicación R.O – 1 – 806 "C" Resumen de disposiciones doctrinarias y de Procedimientos de Comunicaciones Navales;* PCN-3; edición 2010.

Army Technology (2023); *The evolution of military comms: From radios to advanced digital systems*; Recuperado de https://www.army-technology.com

Baigorria, F. (2019); *"Estructura del Sistema de Comando y Control en el Nivel Operacional y los desafíos del siglo XXI";* Trabajo Final Integrador de Especialización; Escuela Superior de Guerra Conjunta; Buenos Aires.

Blanchard, B. S.; Fabrycky, W. J. (2013); *Systems engineering and analysis*; 5ta Edición; Pearson.

Bueno, Francisco José Matías (2019); *Electronic Warfare*; Revista Ejércitos; Recuperado de https://www.revistaejercitos.com/en/articulos/la-guerra-electronica-la-gran-ventaja-rusa/.

Cañete, P. A. (2020); *El comando de ciberdefensa alemán: un claro ejemplo de integración*; Visión Conjunta Nro 22; pp. 17-23.

Carlo Ghezzi, Mehdi Jazayeri, Dino Mandrioli.; *Fundamentals of Software Engineering*; Prentice Hall; Edición 1991.

Cornaglia, Silvina; Vercelli, Ariel (2017); *La ciberdefensa y su regulación legal en Argentina (2006-2015);* Revista Latinoamericana de Estudios de Seguridad, Facultad Latinoamericana de Ciencias Sociales; Nro. 20; pp. 46-62.

Cundins, E. (2020); *El factor militar como medio de prevención pacífica de conflictos*; Visión Conjunta Nro 22; pp. 24-33.

Curtiss-Wright (2024); *MOSA (Modular Open Systems Approach) for military systems*; Recuperado de https://www.curtisswrightds.com

Defense Technical Information Center; *Modular Systems in Military Applications;* Defense Technical Information Center (DTIC); sf; Recuperado de https://www.dtic.mil

Ejército Argentino; *Conducción de las Fuerzas Terrestres;* ROB 00-01; edición 2015.

Ejército Argentino; *Conceptos básicos sobre sistemas de comunicaciones, informática y guerra electrónica;* ROD 05-01; edición 2017.

Fuerza Aérea Argentina; *Reglamento de Conducción Operacional;* RAC-3; edición 2010.

Herrera, L. (2015); *"Diseño y planificación de las actividades de guerra electrónica en el ambiente operacional";* Trabajo Final Integrador de Especialización; Escuela Superior de Guerra Conjunta; Buenos Aires.

Jane's Defence Weekly; *Analysis of Modular Systems in Modern Military Programs;* Jane's Information Group; s.f.; Recuperado de https://www.janes.com

Military & Aerospace Electronics; *Modular Electronics and Their Impact on Military Communication and Radar Systems*; Military & Aerospace Electronics; s.f.; Recuperado de https://www.militaryaerospace.com

Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Planeamiento para la Acción Militar Conjunta. Nivel operacional – Proyecto;* PC 20-01; edición 2023.

Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Doctrina Básica para la Acción Militar Conjunta – Proyecto;* PC 00-01; edición 2023.

Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Comunicaciones para la Acción Militar Conjunta;* PC 16-01*;* edición 2019.

Ministerio de Defensa (2020); Estrategia Nacional de Ciberdefensa; Buenos Aires; Recuperado de https://www.argentina.gob.ar/defensa/ciberdefensa.

Ministerio de Defensa (2017); Resolución Ministerial Nº 504; Norma Def Com 1224; Comunicaciones: Redes tácticas de enlace de datos para el Comando y Control.

Ministerio de Defensa; *Taiana participó de la presentación del ciclo de planeamiento de la Defensa Nacional*; Noticias; Recuperado de https://www.argentina.gob.ar/noticias/taiana-participo-de-la-presentacion-del-ciclo-de-planeamiento-de-la-defensa-nacional

Modern Battlespace (2018); *The demand for military interoperability is resulting in modular comms approaches;* Recuperado de https://www.modernbattlespace.com

Moresi, A. A. (2020); *El conflicto futuro*; Visión Conjunta Nro 22.

Moyano, T. R. (2020); *La República Argentina y sus esfuerzos en ciberdefensa*; Visión Conjunta Nro 22.

Nieto, Ignacio (2023); *¿Por qué lo llamas ciber cuando quieres decir guerra electrónica?*; Global Strategy Report 9/2023; Recuperado de https://global-strategy.org/por-que-lo-llamas-ciber-cuando-quieres-decir-guerra-electronica/.

North Atlantic Treaty Organization (2020); *NATO Modular Combat Vehicles: Flexibility and Adaptability in European Operations;* NATO; Recuperado de https://www.nato.int

North Atlantic Treaty Organization (2021); *NATO Modular Communication Networks: Enhancing Multinational Interoperability*; NATO; Recuperado de https://www.nato.int

Pahl, G., Beitz, W. (1996); *Engineering Design: A Systematic Approach;* Springer-Verlag; Londres.

Policante, P. (2021); *"Diseño de un Sistema de Comunicaciones Interoperable para el Instrumento Militar de la Nación";* Trabajo Final Integrador de Especialización; Escuela Superior de Guerra Conjunta; Buenos Aires.

Ratti, A. (2014); *"Interoperabilidad de los sistemas de comunicaciones en apoyo al comando y control en el nivel estratégico operacional";* Trabajo Final Integrador de Licenciatura; Escuela Superior de Guerra; Buenos Aires.

República Argentina; Ley de Defensa Nacional; Nro. 23554; sancionada el 13 de abril de 1988; promulgada el 26 de abril de 1988.

República Argentina; Ley Restructuración de la Fuerzas Armadas Argentinas; Nro. 24948; sancionada el 18 de marzo de 1998; promulgada el 3 de abril de 1998.

República Argentina; Ley de Seguridad Interior, Nro. 24059; sancionada el 18 de diciembre de 1991, promulgada el 6 de enero de 1992.

República Argentina; Ley de Inteligencia Nacional; Nro. 25520; sancionada el 27 de noviembre de 2001, promulgada el 3 de diciembre de 2001.

República Argentina; Ley de Protección de los Datos Personales, Nro. 25326; sancionada el 4 de octubre de 2000, promulgada el 30 de octubre de 2000.

República Argentina; Ley de Telecomunicaciones, Nro. 19798; sancionada el 22 de agosto de 1972, promulgada el 23 de agosto de 1972.

República Argentina; Ley Delitos Informáticos y Ciberseguridad; Nro. 26388; sancionada el 4 de junio de 2008, promulgada el 24 de junio de 2008.

República Argentina; Ley Incorporación; Nro. 26904; sancionada el 13 de noviembre de 2013, promulgada el 4 de diciembre de 2013.

República Argentina; Decreto 457/21; Directiva de Política de Defensa Nacional (DPDN) 2021.

República Argentina; Decreto 727/06; Reglamentación de la Ley de Defensa Nacional Nro. 23554.

República Argentina; Decreto 1691/06; Directiva sobre la organización y funcionamiento de las fuerzas armadas.

Sommerville, I.; *Ingeniería de Software;* Pearson Educación; México; Año 2011.

U.S. Department of Defense (2018); *Modular Airborne Electronic Warfare Systems: Enhancing Flexibility and Operational Capability*; U.S. Department of Defense; Recuperado de https://www.defense.gov

U.S. Department of Defense (2022); *Cyber Defense Modular Architecture for Rapid Threat Response;* U.S. Department of Defense; Recuperado de https://www.defense.gov.

Videla Solá, Mariano German (2023); *Proyecto de Presupuesto 2024: Las Fuerzas Armadas Argentinas buscan incorporar sistemas de defensa antiaérea de mediano alcance*; Zona Militar; Recuperado de https://www.zona-militar.com/2023/09/20/presupuesto-2024-las-fuerzas-armadas-argentinas-buscan-incorporar-sistemas-de-defensa-antiaerea-de-mediano-alcance/