



Facultad del Ejército
Escuela Superior de Guerra
“Tte Grl Luis María Campos”



TRABAJO FINAL INTEGRADOR

**Título: “Desarrollo de capacidades del Instrumento
Militar Terrestre para operar en un ambiente de la
Guerra de la Información.”**

**Que para acceder al título de Especialista en Conducción Superior de
OOMMTT presenta el Mayor MARIANO AGUSTIN LOSITO.**

Director de TFI: Coronel (R) AGUSTO CAYO.

Ciudad Autónoma de Buenos Aires, de marzo de 2022.

Resumen

Las últimas décadas, el mundo fue testigo del avance vertiginoso de la tecnología en todos los ámbitos y éstas siguen creciendo en proporción geométrica. Las Fuerzas Armadas no fueron ajenas a este avance. El espectro electromagnético y los medios utilizados en él, fueron los que más se desarrollaron en este aspecto, permitiendo al que lo domine, tener una posibilidad cierta de obtener la victoria.

Es así que, logrando los efectos deseados mediante las Operaciones de Información (OI), dará una clara ventaja a quien posea la mejor tecnología, preparación y predisposición.

Precisamente el desarrollo de estas capacidades en el Instrumento Militar Terrestre, es el motivo de la presente investigación.

Para ello, se trazó como objetivo general determinar la estructura de una organización que esté en capacidad de desarrollar las distintas funciones que se deben ejecutar en un ambiente de la Guerra de la Información. Para tal fin se diseñaron tres ejes conceptuales: el primero trata el análisis de distintos escenarios bélicos donde se empleó la Guerra de la Información a los efectos de extraer las enseñanzas pertinentes; en el segundo eje se analizó el marco legal para determinar si existe algún impedimento para realizar tales acciones, como así también, se hicieron comparaciones entre nuestra doctrina con la doctrina de los ejércitos de países regionales y extra regionales; y en un último eje conceptual se precisaron cuáles son los elementos necesarios que deben integrar una organización para operar en un ambiente de la Guerra de la Información a los efectos de diseñar una estructura eficiente a tal fin, ya sea con medios orgánicos existentes y eventualmente con la creación de otros nuevos. La fuente de información para este trabajo se basó en el estudio de la doctrina propia y extranjera, leyes nacionales, datos bibliográficos nacionales y extranjeros, conferencias y entrevistas.

Palabras claves

Guerra de la Información, Netwar, Swarming, Ciberdefensa

ÍNDICE GENERAL

Introducción	1
Presentación del problema:	1
Antecedentes del problema:	1
Marco de referencia para el análisis del problema	4
Justificación del Problema Planteado	5
Objetivos.....	6
Metodología a emplear	7
 Capítulo I: Empleo de las Operaciones de Información en distintos escenarios bélicos...8	
Sección 1: Antecedentes Históricos.	8
Sección 2: Escenarios bélicos recientes.....	11
II da Guerra Mundial (3ra Generación).	11
El caso del Mayor Martin.	12
Operación Fortitude.....	12
Guerras y operaciones entre Árabes e Israelíes (3ra Generación).	13
Guerra de Yom Kipur.	13
Destrucción de un reactor nuclear Sirio por parte de Israel.....	15
Guerra del Golfo (Tormenta del Desierto” 4ta Generación).	17
Guerra de Afganistán Operación Lanza de Neptuno y Eliminación del Grl Qasem Soleimani (5ta Generación).....	18
La operación “Lanza de Neptuno”.	19
Eliminación del Grl Qasem Soleimani.	21
Conclusiones parciales	22
 Capítulo II: Plexo Normativo Nacional y Marco Doctrinario	24
Sección 1: Plexo Normativo Nacional	24

Ley 23.554 de Defensa Nacional	25
Ley 24.059 de Seguridad Interior.....	28
Ley 25.520 de Inteligencia Nacional.....	30
Ley 27.126 Agencia Federal de Inteligencia (AFI).....	31
Comentarios finales respecto al marco legislativo vigente.....	33
Sección 2: Doctrina Propia del Instrumento Militar Terrestre.....	34
Sección 3: Doctrina de potencias mundiales	36
Estados Unidos de Norte América	36
Federación Rusa	37
República Popular China	41
Sección 4: Doctrina en el Marco Regional.	43
Conclusiones parciales	48
Capítulo III: Propuesta de una organización	50
Sección 1: Efectos que se pueden alcanzar con las Operaciones de Información	50
Los efectos pueden ser de dos categorías.	51
Efectos basados en el daño:	51
Efectos basados en su naturaleza.	52
Efectos basados en la interacción del blanco con su entorno o sistema.	52
Sección 2: Elementos idóneos para operar en la Guerra de la Información orgánicos del IMT y a crear.....	53
Orgánicos del IMT.	53
Inteligencia.....	53
Guerra Electrónica.....	53
Tropas de Operaciones Especiales	53

Fuerzas Especiales.....	54
Ciberdefensa.....	54
Elementos a crear o requerir.	54
Centro de asesores comunicacionales y prensa.....	54
Sección 3: Organización de un elemento para la Guerra de la Información.	55
Propuesta de organización de una Célula y su funcionamiento.....	56
Conclusiones parciales	58
Conclusiones finales.....	60
Aporte Profesional.....	64
Referencias.....	66
Anexo 1 (Esquema Gráfico Esquemático)	69
Anexo 2: (Entrevista Nro 1).	70
Anexo 3: (Entrevista Nro 2)	72
Anexo 4: (Entrevista Nro 3).	75
Anexo 5: Influencias de las operaciones durante el conflicto.....	77

Índice de tablas

Cuadro 1. Comparación entre la Doctrina del Ejército de Chile y del Ejército de Brasil.	43
--	----

Índice de Figuras

Figura 1. Propuesta de una Organización para operar en un ambiente de la Guerra de la Información.....	56
--	----

Introducción

Presentación del problema:

¿Cuál es el diseño más apto de una organización en el marco del IMT a nivel operacional, para operar en un ambiente de la Guerra de la Información?

Antecedentes del problema:

La presente investigación sienta sus bases en la necesidad que tiene un comandante para anticiparse y crear las condiciones necesarias para desarrollar operaciones eficaces a fin de obtener el estado final deseado.

Éste precisamente es el objetivo que busca la Guerra de la Información.

Lo primero que debemos hacer es definirla. Sobre el particular existen diferentes acepciones, entre las cuales las más destacadas son las siguientes:

Guerra de la Información es el uso y manejo de la información con el objetivo de conseguir una ventaja decisiva sobre el enemigo, pudiendo abarcar tanto la obtención de información táctica y la confirmación de su veracidad, como la desinformación, a efectos de afectar las operaciones del enemigo, socavando la calidad de información obtenida por éste y negándole la oportunidad de búsqueda y reunión de información (Ejército Argentino, Conducción para las Fuerzas Terrestres (ROB - 00 - 01), 2015, pág. 8).

Son las acciones que se llevan a cabo para obtener la superioridad en todo lo que afecta a la información, así también como a su procesamiento, sus sistemas de información y protección de las redes de computación propias y de las acciones del adversario. (Ferrari, Vigón, Gaggero, 2001, pág. 35).

Guerra de la Información consiste en el uso ofensivo y defensivo de la información y de los sistemas de información para negar, explorar, corromper o destruir la información del adversario, su proceso de información, los sistemas de información

y las redes de computación mientras se procura la protección de los propios sistemas (Ferrari, Vigón, Gaggero, 2001, pág. 35).

“Son acciones tomadas para afectar e influir los procesos de toma de decisiones, información, y sistemas de información del adversario y otras entidades mientras que se protege su propia información y sistemas de información” (Campos, 2021).

De acuerdo al último autor citado, los Niveles de Guerra de la Información son:

Tipo I: Manipular percepciones, a través de operaciones de engaño; operaciones psicológicas y otras técnicas; proteger de los esfuerzos del enemigo por manipular las propias percepciones.

Tipo II: Negar, destruir, degradar o distorsionar los flujos de información del enemigo, con el objeto de desarticular sus organizaciones y limitar su habilidad para coordinar operaciones. Abarca acciones físicas, de Guerra Electrónica (GE), o cualquier técnica diseñada para negar la información o funciones de información a quien lo necesita.

Tipo III: Reunir información explotando el empleo por parte del enemigo de sus sistemas de información. Implica la protección de los propios sistemas (Campos, 2021).

Dentro de estas definiciones anteriormente nombradas se desprenden las operaciones que proporcionan el núcleo duro de la Guerra de la Información a saber:

- a. Ciberwar (Arquilla, Ronfeldt, 1993)
- b. Netwar (Arquilla, Ronfeldt, 2001)
- c. Swarming (Arquilla, Ronfeldt, 2001) (Campos, 2021).

“La guerra de información puede adoptar diversas formas:

- Las transmisiones de televisión, Internet y radio pueden bloquearse.
- Las transmisiones de televisión, Internet y radio pueden ser secuestradas para una campaña de desinformación.
- Las redes logísticas pueden desactivarse.

- Las redes de comunicaciones enemigas pueden desactivarse o falsificarse, especialmente la comunidad social en línea en la actualidad.
- Las transacciones bursátiles pueden ser saboteadas , ya sea con intervención electrónica, filtrando información sensible o colocando desinformación.
- El uso de drones y otros robots de vigilancia o cámaras web.
- Gestión de la comunicación” (Wikipedia, Information warfare, 2021).

Las Operaciones de Información no solamente actúan sobre objetivos duros, sino que también sobre objetivo blandos, y en estos últimos haciendo énfasis sobre la voluntad de enemigo y quebrar su espíritu de lucha. Estas acciones se logran en principio preservando el poder de combate propio, y dentro del arte operacional es alterar el ritmo de las operaciones, logrando de esta manera que el enemigo se adapte y siga la secuencia normal de las operaciones, quien logre este desconcierto donde uno se empieza a preguntar ¿Qué ocurre?, ¿Por qué ocurre?¿que vendrá ahora?, logra afectar significativamente la toma decisiones del adversario, obteniendo que en forma repetitiva tome decisiones que afecten su funcionamiento sistémico.

Teniendo una aproximación de definiciones y sus posibles métodos de acción, es oportuno establecer en qué momento se van a desarrollar estas operaciones y en qué momento tendrán preponderancia con mayor intensidad durante la concreción del efecto final deseado que va a constituirse como sinergia para obtener la victoria. (Ver Anexo 5)

Los antecedentes de la Guerra de la Información son difusos y remotos ya que sus métodos fueron empleados en distintos tiempos y escenarios a través de la historia de guerra de la humanidad, pero como tal, tuvo su epicentro en la Guerra del Golfo “Tormenta del Desierto” (02 Ago90/28 Feb91). En ese entonces el mundo fue testigo a través de los medios de comunicación, de cómo el General Herbert Norman Schwarzkopf ofrecía diarias conferencias al públicas, mostrando el poderío bélico norteamericano y el avance de las operaciones. Se pudieron observar, entre otras cosas, los misiles cruceros Tomahawk destruyendo los medios

de comunicación y puestos de observación iraquíes previo a iniciar las operaciones. De esa manera, elevaba sin dudas la moral de la tropa, conseguía adhesión de la propia población y causaba efectos negativos sobre el espíritu de lucha del enemigo junto a su destrucción material.

A partir de ese momento la Guerra de la Información se transformó en una realidad a través de diversos medios, como el proyecto combinado entre norteamericanos y británicos para insertar virus informáticos en la red de comando y control de Saddam Hussein; la penetración de 34 centros militares norteamericanos por 5 hackers desde Holanda entre abril 1990 y marzo de 1991 para vender esa información a Iraq durante la guerra del Golfo; el robo del código de un programa de guía de misiles de la marina de los Estados Unidos de Norteamérica por parte de un hacker según el diario Clarín del 04 marzo del 2001; el uso intensivo de los medios de comunicación por parte de Irak como de los Estados Unidos de Norteamérica para influenciar la opinión pública, entre otros. (Clarín, 2021)

Desde ese entonces hasta la fecha pasando por el 11 septiembre del 2001, a la que se denominó la 2da Guerra de la Información, se viene desarrollando y perfeccionando este tipo de estrategia como una herramienta eficaz para la disuasión y/o persuasión de la fuerza oponente, coadyuvando así a la consecución de los objetivos que se fija el comandante.

Marco de referencia para el análisis del problema

En el continente americano, el país más avanzado en el empleo de la Guerra de la Información son los Estados Unidos de Norteamérica, la cual viene empleando en los distintos escenarios donde ha tenido que actuar. Para ello ha desarrollado una abundante doctrina tanto específica como conjunta la cual está en permanente actualización sirviendo de referencia a otros países integrantes de la Organización del Tratado del Atlántico Norte (OTAN) como así también de los países en el marco regional.

Si bien ningún país tiene una postura oficial sobre este tipo de operaciones, es importante mencionar que la información se utiliza como un tipo de arma incruenta, para el

logro de un Estado Final Deseado Militar/Operacional. Esta información podrá en su evolución adoptar un carácter ofensivo y defensivo que posteriormente se transformará en objetivos militares, que se alcanzan a través del empleo del instrumento militar, afectando significativamente sus funciones de combate, principalmente su capacidad del comando y control, el acceso a la toma de decisiones y el empleo de sistema de armas (Tovar, 2021).

Teniendo en cuenta que si el principal socio de la OTAN, Estados Unidos de Norteamérica (EEUU), tiene desarrollado y normado este tipo de operaciones, cabe inferir, que lo propio habrán hecho sus aliados, por lo tanto, concluimos que los principales ejércitos del mundo contemplan la Guerra de la Información como una herramienta para el logro de sus objetivos operacionales.

En el marco regional países vecinos como la República Federativa de Brasil y la República de Chile, incluyen estas operaciones en su plataforma doctrinaria, con una clara influencia de la doctrina de la OTAN.

Justificación del Problema Planteado

En nuestro caso particular la Guerra de la Información no pasa inadvertida, se la menciona como tal en el ROB 00-01 “Conducción de la Fuerzas Terrestres” en el Cap II “Las Fuerzas Terrestres” al momento de hablar en la Sec II de las “Funciones de Combate” y en particular en su art. 2009 “Inteligencia” donde incluso la define, y en el Cap VII “Operaciones Complementarias” cuando en sus Secciones VIII “Inteligencia”, IX “COSACO” y XV “Ciberdefensa”, aclaran en sus últimos párrafos, que:

“(…) integran el conjunto de las operaciones que conforman la Guerra de la Información, contribuyendo a la obtención de los objetivos / finalidad que persigue la misma” (Ejército Argentino, Conducción para las Fuerzas Terrestres (ROB - 00 - 01), 2015, pág. 27)

Por lo expuesto queda claro que, si bien nuestra doctrina contempla la Guerra de la Información, sin embargo, no aclara cuales son las operaciones a desarrollar, como así tampoco,

las organizaciones más aptas existentes o a crear para llevarlas a cabo, ni sienta las bases para el desarrollo de una doctrina derivada particular de este tipo de guerra.

Podemos advertir por lo tanto que la Guerra de la Información es una herramienta valiosa a la hora de entrar en operaciones y que en el ámbito regional/ internacional hay países que desarrollaron esta doctrina. La ausencia del propio desarrollo en tal sentido, crea una vulnerabilidad en nuestras capacidades para eventualmente intervenir en las guerras actuales.

Objetivos.

Objetivo general. Determinar la estructura de una organización del IMT a nivel operacional, para desarrollar las distintas funciones que debe ejecutar en un ambiente de la Guerra de la Información.

Objetivos Específicos.

Objetivo Específico 1. Analizar los principales escenarios bélicos en un ambiente de 3ra, 4ta y 5ta generación, para determinar el empleo de la Guerra de Información en ellos y que operaciones las materializaron.

Objetivo Específico 2. Analizar datos bibliográficos y la doctrina vigente en el propio IMT y en el de otros países en el marco regional (República Federativa de Brasil y República de Chile) y principales potencias mundiales (Estados Unidos de Norte América, Federación de Rusia y República Popular China) referido a la Guerra de la Información, como así también el ordenamiento legal argentino, para determinar si este tipo de guerra, encuentra impedimento de empleo

Objetivo Específico 3. Precisar cuáles son los elementos necesarios que deben integrar una organización para operar en un ambiente de la Guerra de la Información a nivel operacional a los efectos de diseñar una estructura eficiente a tal fin, a la luz de las disponibilidades actuales del IMT y eventualmente determinar la necesidad de la creación de nuevos elementos.

Metodología a emplear

La presente investigación se desarrollará sobre la base del método deductivo, en la cual se plantea un objetivo general y tres objetivos específicos, de los cuales se desarrollarán conclusiones parciales para dar respuestas a cada uno de los objetivos particulares, y posteriormente, conclusiones finales las cuales brindarán las respuestas al objetivo general planteado en la presente investigación.

El diseño de la investigación será de carácter explicativo, en el cual se empleará como técnica de validación el análisis bibliográfico, documental, lógico y entrevistas. El esquema metodológico a emplear está detallado en el Anexo 1 a la presente investigación.

El presente trabajo se desarrollará en tres capítulos. El primer capítulo tendrá por objeto realizar un análisis de los escenarios bélicos donde se utilizaron este tipo de operaciones, para determinar en cuáles de ellos fueron utilizadas. El segundo capítulo se analizará en su primer primera el marco legal, y posteriormente se enfocará en el análisis de la doctrina propia como así también la del marco regional (Chile Y Brasil) y en el de las potencias mundiales (Estados Unidos de Norteamérica, Rusia, China). En el tercer capítulo se buscará diseñar un sistema eficiente para operar en este tipo de ambiente, para finalmente poder extraer las conclusiones finales de la investigación.

Capítulo I: Empleo de las Operaciones de Información en distintos escenarios bélicos

Hit first! Hit hard! Keep on hitting!” (golpea primero, golpea fuerte, continúa golpeando). (Admiral Sir John Fisher, 1919).

El propósito de este capítulo es analizar distintos escenarios bélicos de 3ra, 4ta y 5ta generación para determinar en cuáles de ellos se empleó la Guerra de Información y qué operaciones la conformaron.

Los rasgos geopolíticos de los conflictos armados surgen al finalizar la guerra Franco-Prusiana y la declaración de la Paz de Westfalia en 1648, en donde se empieza a contener a los diferentes imperios que trataban de expandir su zona vital, dando los conceptos que hoy conocemos de Hinterland, frontera, núcleo vital, entre otros, que trajo en consecuencia una clasificación de las distintas generaciones de la guerra según los hechos históricos del momento que hicieron un cambio de paradigma significativo.

Es importante aclarar que los escenarios de 3ra generación son aquellas que se realizan más por maniobras que por fuerzas de gran magnitud, este concepto surge en Alemania, y se la conoce como Guerra de Maniobras o Guerra Relámpago (Blitzkrieg). Las de 4ta generación se dan en un marco asimétrico de fuerzas, y llevado adelante entre fuerzas regulares contra guerrillas, utilizando tácticas y procedimientos de empleo no convencionales. De la misma manera haremos mención a los escenarios de 5ta generación que marca su evolución a través de la implementación de nueva tecnología. (Ejército Argentino, Especialización en Historia Militar Contemporánea, 2020)

Sección 1: Antecedentes Históricos.

La Guerra de la Información (no con esa denominación), es tan antigua como la humanidad y la misma guerra, por la sencilla razón de que la información - y la inteligencia derivada en muchos casos - es sencillamente poder que a su vez es sinónimo de potencia, energía y dominio.

La llamada Guerra de la Información ha sido usada entonces desde tiempo milenarios, podemos mencionar como ejemplo algunos de los principios o axiomas del General y Filósofo chino Sun Tzú para confirmarlo. Muchos autores han seleccionado entre veintiuno a veinticuatro como los más importantes, acotándonos para esta investigación, a los que tienen una relación directa con la información, veámoslos:

1. «El arte de la guerra es someter al enemigo sin luchar».
2. «Conoce al adversario y sobre todo concóctete a ti mismo y serás invencible».
3. «Conoce a tu oponente, concóctete a ti mismo y no pondrás en peligro tu victoria».
4. «Conoce el cielo y conoce la tierra, y tu victoria será total».
5. «Si no te conoces a ti mismo ni a tu oponente, en cada batalla serás derrotado».
6. «Ganar cien veces en cien batallas no es el apogeo de la habilidad. Someter al enemigo sin pelear es el apogeo de la habilidad».
7. «Todo arte de la guerra se basa en el engaño».
8. «Debemos fingir debilidad, para que el enemigo se pierda en la arrogancia».
9. «Mantén a tus amigos cerca y a tus enemigos aún más cerca».
10. «Llévalos a un punto del que no puedan salir, y morirán antes de poder escapar».
11. «Grandes resultados pueden ser conseguidos con pequeños esfuerzos».
12. «Si haces que los adversarios no sepan el lugar y la fecha de la batalla, siempre puedes vencer». (Sun Tzu, 2014, pág. 7)

Someter sin luchar - el primero - sólo se logra con información e inteligencia y mentalidad estratégica siendo la astucia (habilidad para comprender las cosas y obtener provecho o beneficio mediante engaño o evitándolo) la principal herramienta del conductor.

Las tres siguientes hacen al conocimiento de los principales ámbitos de los escenarios de la guerra que más nos interesan y que traducidos a nuestro lenguaje actual equivaldrían a terreno, enemigo, condiciones meteorológicas y personalidades.

Los subsiguientes hacen mención al engaño

Sólo han variado, al transcurrir los tiempos, los métodos. Según el General de División José Carlos Albano do Amarante (ingeniero brasilero) en su libro “El vuelo de la humanidad” menciona que:

“(…) en el comienzo del ciclo de la Revolución Industrial entre 1750 y 1850 se produjo una transición de tecnologías de base empírica hacia tecnología de base científica(…)” (Do Amarante, 2014, pág. 67)

Yendo así por ejemplo de la máquina a vapor a la de combustión interna. Pero, sigue el mismo autor :

“(…)en los dos ciclos siguientes, entre 1850 y 1940, fruto de un crecimiento científico acelerado, la ciencia sobrepasó a la tecnología y las invenciones pasaron a tener fundamento científico, como fueron el reloj de cuarzo, el misil intercontinental (…)” (Do Amarante, 2014, pág. 72)

Culmina esta explicación con un cuadro donde muestra que las llamadas “tecnología de impacto” o de repercusión social mundial tuvieron su mayor desarrollo entre los años 1940 al 2000 y continúan. Entre el año 8000 AC y el 1000 DC dichas tecnologías se cuantifican sólo en 20 y a partir de mediados del Siglo XX crecen hasta alcanzar el número de 120.

¿A dónde se pretende llegar con lo anterior? A sostener que la Guerra de la Información no sólo siempre existió, sino que con el tiempo y el desarrollo de tecnologías de crecimiento acelerado solo se ha perfeccionado buscando resultados más rápidos, pero - también - con una limitación: la capacidad humana de procesar y utilizar la voluminosa información que se obtiene.

Yendo al tema del capítulo se puede observar que también tiene gran relación con lo dicho por el General Do Amarante, pues el crecimiento tecnológico de alto impacto como lo llama él, toma nuestro tema: los escenarios de 3ra, 4ta y 5ta generación, desde la Segunda

Guerra Mundial hasta nuestros días. Es claramente que en ese lapso se da el gran salto tecnológico en armas, comunicaciones, medios de obtención de información. Tan grande es este paso que impone el establecimiento de organismos o agencias específicas para su empleo surgiendo también el problema de la coordinación con otros.

Sección 2: Escenarios bélicos recientes.

Los escenarios bélicos desde la II Guerra Mundial hasta la fecha son muy numerosos superando 150 desde 1939 con la invasión a Polonia hasta el conflicto recientemente finalizado en Afganistán.

Los escenarios son variados, los protagonistas también pues incluyen desde uniformados regulares hasta irregulares, terroristas y narcoterroristas. Respecto a los escenarios podemos citar el renombrado “11S” y el inmediato ataque a Afganistán y cabría analizar si el ataque en territorio norteamericano fue un acto “terrorista” o de guerra, pero eso daría mucho para hablar.

Como sea, largo sería enumerar cada uno de los casos; se ha optado entonces por mencionar las operaciones de la II Guerra Mundial, las Guerras Árabes Israelíes, la Guerra del Golfo a modo de ejemplo y Afganistán.

II da Guerra Mundial (3ra Generación). Francia e Inglaterra parecían “no creer” en lo que haría Alemania a partir de la asunción de Hitler al poder, sólo pocas voces no escuchadas alertaron sobre lo que podría ocurrir y que ocurrió. Invadida Francia por Alemania el aislamiento informativo de los ingleses y otros aliados era tremendo, patético. Desconocían casi todo lo que disponían las FFAA alemanas y la potencia y la astucia germánica se combinaron usando y disponiendo de superioridad de información para abalanzarse hacia el Este.

Surge entonces la necesidad en el cabal sentido del término de organizar y desplegar una red de espionaje para reunir información y otras tareas también relevantes de sabotajes, organizar la llamada “resistencia”, infiltrarse y comunicarse con Londres. Esa necesidad se

cubrió con la creación del S.O.E. (“Special Operati3n Executive”) cuyos Jefes primeros fueron el General de Divisi3n Sir Colin Gubbins y el General R.H. Barry. Al comenzar a formarse a fines de 1940 la carencia de informaci3n sobre lo que acontecía en Francia era alarmante y poco tiempo despu3s el S.O.E. comenz3 a enviar a sus agentes con dos misiones principales: Verificar si había alguna organizaci3n de resistencia en Francia y apoyarla con armas, organizaci3n, explosivos, extender la red y la segunda informar a Londres sobre todo lo que fuera pertinente a la guerra, desde la vida de la gente hasta los movimientos de tropas.

Las operaciones realizadas dentro de nuestro tema de Guerra Informativa que pueden citarse, entre otras, fueron:

El caso del Mayor Martin. Consistió en el abandono un cadáver en la costa española cerca de Gibraltar donde se sabía de la existencia de agentes alemanes, el objetivo era engañar a los alemanes sobre el desembarco aliado en Sicilia, haciéndoles creer que sería en Grecia y Cerdeña. El 30 de abril de 1943 fue encontrado por un pescador de Huelva (España) el cadáver con la documentaci3n de engaño. La documentaci3n fue prestada por los españoles a los alemanes quienes tomaron copia, y luego fue devuelta pues era reclamada por Inglaterra. Los aliados invadieron Sicilia el 11 de julio de 1943 ante unos alemanes consternados que habían cambiado sus tropas de lugar. (Infobae, 2021)

Operaci3n Fortitude. Conjunto de operaciones tácticas para engañar a los alemanes sobre el lugar de desembarco de las Fuerzas Aliadas en la costa francesa. Incluy3: infiltraci3n de comandos en Francia, desembarco de tropas en Dieppe, reconocimiento minucioso de playas de desembarco, transmisi3n de informaci3n sobre las defensas alemanas y su capacidad real, ubicaci3n y movimientos de tropas alemanas hacia la costa, lanzamiento de radios emisoras que operaban en frecuencias alemanas, transmisiones de desinformaci3n, envío de un “doble” del Mariscal Montgomery a Gibraltar que difundió la informaci3n que invadirían por el Sur de Francia. Con esas operaciones de informaci3n se continuó hasta el mismo 6 de junio de 1944

en que se lanzaron muñecos paracaidistas entre El Havre y Boulogne Sur - Mer y se lanzaron bombarderos sobre esa misma zona. Mientras Rommel se encontraba en su hogar en Alemania llevando unos zapatos de regalo a su esposa - enterado del desembarco regresó - los alemanes seguían creyendo que el desembarco en Normandía era una maniobra de distracción. (Capanegra, Julian, 2021)

Guerras y operaciones entre Árabes e Israelíes (3ra Generación).

Guerra de Yom Kipur. La guerra de Yom Kipur en 1973, formó parte del conflicto entre árabes e israelíes como uno de los tantos encuentros que tuvieron ambos desde la formación del Estado Israelí en 1948. Cabe recordar que, en la llamada guerra de los Seis Días en 1967, Israel obtuvo los Altos del Golán de Siria y la península de Sinaí de Egipto, con lo cual quedaba abierta una herida que dio pie a la guerra que nos ocupa.

La recuperación de las tierras perdidas, fue un objetivo para Egipto y Siria, a tal punto que pocos meses después de la finalización de los Seis Días, la Cumbre Árabe de Jartum, en septiembre de 1967, emitió lo “tres no”: no a la paz con Israel, no al reconocimiento, no a la negociación, por lo cual, Israel comenzó a reforzar sus fronteras a lo largo del canal de Suez. Por su parte los estados árabes comenzaron su refuerzo armamentístico con el apoyo de la Unión Soviética mientras que en el seno de la Organización de las Naciones Unidas se realizaban vanos esfuerzos para evitar la guerra.

El presidente egipcio Sadat, si bien propuso para lograr un pacto de no beligerancia el retiro de las tropas israelíes de las tierras ocupadas en la guerra de los Seis Días, ya estaba decidido a solucionar la crisis por medio de las armas.

Egipto expulsó en 1972 a 20.000 asesores militares soviéticos, dando a Israel la falsa percepción de una debilidad en las fuerzas armadas egipcias. Así mismo, la exitosa acción de prensa de Sadat amenazando constantemente a Israel con el inicio de la guerra, también contribuyó a que se creyera no solo por Israel, sino que también por los Estados Unidos, que

esta no se concretaría. La planificación para la guerra junto a Siria, llamado en código Operación Badr (en árabe luna llena) había comenzado un año antes.

Israel, a mediados del año 1973, a través de la Dirección de Inteligencia Militar (Aman) y del Departamento de Investigación de las Fuerzas de Defensa de Israel (FDI), estaban al tanto de los planes árabes, pero veían poco probable que se concretara. Es evidente que las Operaciones de Información en la cual actuaba, la prensa, el velo y engaño y la desinformación, ponía a Israel, en una situación de desventaja frente al futuro agresor. Egipto especialmente se abocó a transmitir una fluida corriente de desinformación o falsa información, especialmente sobre la falta de suministros, deficiente mantenimiento, falta de personal especializado para el manejo de armamentos avanzados, falta de repuestos, etc. que reforzaban la creencia en los israelíes que la guerra estaba lejos de concretarse.

En mayo y agosto de 1973, las fuerzas árabes, llevaron a cabo varias ejercitaciones a gran escala, llegando hasta el canal de Suez, para luego retirarse, obligando a Israel, a movilizar sus fuerzas, con el consiguiente desgaste físico, pecuniario y moral.

La semana previa al Yom Kipur, los egipcios realizaron otro de sus entrenamientos cercanos al canal de Suez, pero esta vez con tropas sirias, lo cual no llamó la atención a Israel, más allá de lo que había ocurrido tantas veces antes, pero esta vez no sería un ejercicio.

El momento elegido para la invasión fue precisamente el día de Yom Kipur, que es el día más sagrado del año judío, día de oraciones para la expiación, coincidente también con el mes musulmán de Ramadán, mes religioso de ayuno y abstinencia, con lo cual reforzaba la creencia que la invasión, al menos en esos días, no se efectivizaría.

La ofensiva egipcia tomó por sorpresa a los israelíes incluso a los Estados Unidos gracias a sus esfuerzos llevados a cabo por las Operaciones de Información. El ataque fue precedido por aproximadamente 150 acciones de engaño tanto políticas como militares. Un equipo especial de 40 integrantes comenzó a planificar en febrero de 1971 el plan para la

invasión de octubre. Este planeamiento incluyó actividades de construcciones simuladas, informes falsos y otras actividades no relacionadas al combate.

En este caso, los egipcios llevaron a los israelíes al borde de la derrota. que luego supieron revertir. Pero queda a la vista como se logró la ventaja de la sorpresa estratégica con la ayuda de un buen plan de Operaciones de Información, con la consiguiente victoria en las primeras fases del plan de campaña que luego no pudieron sostener los árabes por otras razones.

Este sistemático plan de desinformación llevado a cabo por los árabes, ocasionó que el día en que los árabes cruzaron ofensivamente el canal de Suez con 100.000 soldados, 1350 tanques, 2000 cañones y morteros, solo hubiese en la línea de defensa, 450 soldados de la Brigada de Jerusalén y una sola de las tres brigadas blindadas. (Wikipedia, Guerra de Yom Kipur, 2021).

Destrucción de un reactor nuclear Sirio por parte de Israel. Un ciberataque en este milenio, ocurrió el 06 de septiembre de 2007, cuando fuerzas israelíes, destruyeron en territorio sirio, un reactor nuclear que estaba construyendo secretamente con la colaboración de Corea del Norte.

“Acompañando el ataque, hubo un ciberataque a las defensas aéreas de Siria que los dejó ciegos al ataque del reactor nuclear, permitiendo que ocurriera el ataque” (BBC, NEWS, 2021)

Esta operación ejecutada exitosamente por la fuerza aérea y el ejército conjuntamente con las agencias de inteligencia israelíes, representó, sin embargo, un fallo de estos últimos, al no advertir que durante años el país vecino estaba construyendo un reactor nuclear. Después de un mes y medio de investigaciones, el Mossad, concluyó en 2004 que Siria estaba trabajando en un plan nuclear.

“Teníamos imágenes satelitales de un gran edificio en el medio del desierto, sin ninguna explicación “, dice el jefe de MI (inteligencia militar) en ese momento, general (res.) Amos Yadlin.

La confirmación de esta construcción se materializó en Viena, cuando una célula del Mossad, incursionó en el hotel donde se alojaba Ibrahim Othman, jefe de la Comisión de Energía Atómica de Siria que había concurrido a esa ciudad para participar en las deliberaciones de la Agencia Internacional de Energía Atómica. Según la investigación del periodista estadounidense David Masovsky que publicó en The New Yorker en 2012, la célula del Mossad entró en la habitación de Othman, y “limpió” en menos de una hora la computadora personal del funcionario sirio que la había dejado ahí, mientras participaba de la conferencia.

Gracias a esa falla de seguridad, donde se obtuvieron 35 fotos del reactor plutógeno en avanzado estado de construcción, se resolvió realizar la operación de destrucción del mismo.

La operación se planificó en el más absoluto secreto, incluso los pilotos que participarían no sabían sobre la naturaleza del objetivo.

Para el mantenimiento del secreto, se montó una falsa narrativa para la mayoría de los comandantes, para el público y los medios, a través de un minucioso plan de comunicación social.

La fuerza aérea, realizó numerosas maniobras simuladas, la última de ellas fue el martes 04 de setiembre. Los pilotos fueron informados sobre el objetivo a atacar momentos antes del despegue, al igual que las tropas que participaron en la Operación Rosario, que fueron informadas momentos antes del desembarco del 02 de abril de 1982, que el objetivo sería recuperar las Islas Malvinas

Según David Makovsky, investigador del Instituto Washington para Política del Cercano Oriente, además de ocho aviones de ataque, otros aviones también participaron en la

operación. Los aviones despegaron de Ramón y Hatzerim y se dirigieron hacia el norte a lo largo de la costa del Mediterráneo, con amplio uso de la guerra electrónica como camuflaje.

Los ocho aviones descargaron con precisión sus bombas sobre el objetivo el viernes 06 de setiembre de 2007 a las 12:25 a.m. sin ninguna resistencia siria ya que el ataque los tomó por sorpresa

Dice el coronel Amir, piloto de F-15 que participó en el ataque. “Para mí, hoy se conecta con nuestra capacidad de eliminar amenazas en países distantes en el tercer círculo [es decir, Irán]. Desde el ataque en Siria también hemos mejorado maravillosamente, en inteligencia, en nuestro rango de acción, en nuestra capacidad para atacar en secreto (Schnessel, 2021)

En esta acción confluyen varias Operaciones de información para que el efecto deseado fuera obtenido plenamente.

Para asegurar el secreto, se difundieron al público interno y externo falsas informaciones usando los medios de comunicación social, se usaron imágenes satelitales para fotografiar el objetivo, se realizaron ejercitaciones simuladas para no alertar al enemigo sobre el verdadero objetivo, se hizo uso de la guerra electrónica cuando despegaron aviones hacia otro rumbo para no llamar la atención sobre el verdadero rumbo a tomar, se realizaron incursión de inteligencia para capturar información vital sobre el reactor nuclear. Como corolario de todas estas operaciones, se pudieron descargar las bombas que destruyeron el objetivo, sin ningún tipo de impedimento ni reacción inmediata posterior.

Guerra del Golfo (Tormenta del Desierto” 4ta Generación). Este conflicto duró aproximadamente seis meses contando desde la invasión de Irak a Kuwait el 2 de agosto de 1990; La ofensiva de la coalición autorizada por las Naciones Unidas atacó recién el 16 de enero de 1991 y completó la campaña a fin de ese mes. La ONU había dado plazo hasta el 15 de enero de 1991 a Iraq para retirarse. Si bien el comandante era el Príncipe Saudí Khaled bin Sultán el verdadero poder lo ejercía Estados Unidos.

Desde el punto de vista de la información o Guerra de la Información fue un conflicto interesante y hasta curioso ya que la coalición mantuvo y difundió en forma abierta los pasos que iban dando - obviamente con límites -, así es que fue anunciando el traslado de tropas, sus supuestas concentraciones, detalles de algunas armas y hasta la fecha y hora en que atacaría. Por la diferencia horaria la Cable News Network (CNN) mostraba al Presidente Bush caminando a la luz del día por los jardines de la Casa Blanca horas antes de dar la orden de atacar, en actitud meditativa.

Pero bajo toda esa estructura o escenografía se movían satélites, agentes en el terreno, observadores adelantados infiltrados, balizas señaladores de blancos e infiltraciones para obtener información y realizar acciones sabotaje a cargo de escasa, pero muy bien entrenada tropa: el Escuadrón “B” del Special Air Service (SAS) inglés y las Fuerzas Especiales de los EEUU.

La “Masa” principio esencial norteamericano junto a la información difundida al mundo que aceptó el conflicto como una guerra justa, la precisa información sobre blancos, la guerra electrónica, el control de las comunicaciones iraqués, los engaños sobre el lugar del ataque principal permitieron una rápida victoria.

Guerra de Afganistán Operación Lanza de Neptuno y Eliminación del Grl Qasem Soleimani (5ta Generación). Previo analizar la operación en sí, es importante nombrar algunos factores y principios para la conducción de las Operaciones de Información que materializan hoy en día a las mismas.

Fueron extraídas del manual de operación de información de la República de Chile (Ejército de Chile, 2010).

Los principales factores de éxito de las Operaciones de Información son: Inteligencia, tecnología y medios específicos de equipamiento, selección del personal y entrenamiento conjunto.

Los principios que rigen estas operaciones son: si bien todas las operaciones se rigen por principios que guían el cumplimiento de la misión, las Operaciones de Información tienen las propias. Entendiendo a éstos como criterios y estándares de este tema específico que representan una herramienta importante de la cual se nutre el comandante al momento de visualizar el diseño operacional, a continuación nombraremos las de más relevancia: (Stella, Facundo, 2015).

Dirección del mando y su implicación personal: el nivel más adecuado para dirigir y controlar el esfuerzo de estas actividades es el Operacional, teniendo en cuenta alcanzar el Estado Final Deseado por los niveles superiores.

Coordinación estrecha: Las Operaciones de Información requieren una estrecha integración con las otras áreas de la conducción, al igual que los elementos constitutivos de dicha estructura. De tal forma que se pueda sincronizar y coordinar meticulosamente con respecto a las operaciones y otras acciones que se desarrollen en el Ambiente Operacional, evitando que las OI no interfieran o afecten con otras operaciones militares.

Información e inteligencia precisa: Si bien en todas las operaciones es vital contar con la suficiente información en tiempo y forma, en este tipo en particular, cobra mayor relevancia ya que su oportunidad y precisión va a condicionar el planeamiento.

Planificación basada en efectos: al momento de llegar el efecto a lograr, solicitados por los distintos elementos, que pueden ser tanto de acción letal o no letales, buscando la inutilización, neutralización, negación de información y acción comunicacional, entre otros. El jefe de la estructura de Operaciones de Información evaluara con que elemento puede cumplir dicho efecto buscando siempre la economía de esfuerzo y la eficiencia de empleo, como así también, el seguimiento del efecto a lograr, en qué grado se cumplió (Ejército de Chile, 2010).

La operación "Lanza de Neptuno". Luego del 11 de septiembre del 2011, ocurre uno de los acontecimientos terroristas más mortíferos hasta nuestros días, el presidente de ese

entonces George W. Bush, se comprometió ante el mundo a tomar venganza por lo ocurrido, para eliminar a los principales líderes de Al Qaeda y derrocar al gobierno Talibán, lanzando días después la Operación Libertad Duradera (Operation Enduring Freedom). Previo a esto, se infiltraron doce hombres del grupo especial Air and Land Seal Teams (SEAL) juntos con miembros de la Central Intelligence Agency (CIA) con la finalidad de crear las condiciones necesarias para que, ingrese posteriormente el grueso de las fuerzas de propósito general. La misión principal era destruir los campos terroristas mediante fuego aéreo y consolidar la alianza del norte.

La búsqueda de Bin Laden se hacía cada vez más difícil, el momento más cerca de su captura fue en la localidad de Tora Bora, lugar que fue preparado por el grupo extremista durante diez años previos a la invasión. EL líder del grupo oriundo de Arabia Saudita, fue constantemente cambiado de lugares, pasando por Sudán, Afganistán y Finalmente Pakistán.

Durante 11 largos años, todos los grupos de Inteligencias americanos y sus aliados, hicieron su máximo esfuerzo para dar con su paradero, utilizando todos los medios tecnológicos a disposición, agentes infiltrados, fotografía aérea, uso de distintas ONG para intentar confirmar su presencia, escuchas telefónicas, panfleteo de publicidades y propagandas, entrevistas a otros líderes locales y otras acciones relacionadas con las Operaciones de Información.

La operación tuvo lugar el 2 de mayo de 2011, en la localidad de Abbottabad, Pakistán lugar donde un grupo del DEVGRU, perteneciente al grupo SEAL, realizó una Incursión, materializa por una infiltración aérea con helicópteros (Nighth Stalkers), ejecutando un golpe de mano para eliminar al líder de Al Qaeda y capturar toda la información posible y posteriormente una exfiltración aérea hasta Afganistán. La operación fue monitoreada desde la más alta conducción, Estrategia Nacional; encabezada por el Presidente de la Nación y un mando de Operaciones Especiales desde Afganistán en coordinación con la CIA.

En esta operación surgen a la vista un sin números de operaciones de configuración que permitieron a la operación principal (eficaz) llevar a cabo su efecto deseado principal, de las cuales relacionadas a nuestra temática podemos nombrar, guerra electrónica para interceptar los radares enemigo de principalmente de Pakistán, infiltración de fuerzas especiales para confirmar la presencia del objetivo de alto valor, medidas de velo y engaño, traductores para contener a la población que quisiera acercarse, corresponsales de guerra para documentar la secuencia estipulada, entrevistas a prisioneros de guerra que poseían valiosa información. A las claras queda a la vista la importancia de contar con una estructura de esta naturaleza que nos permitirá seleccionar el mejor modo al problema militar operativo (Stella, Facundo, 2015), (Owen, Mark, 2012).

Eliminación del Grl Qasem Soleimani. El de 3 de enero del 2020, en el aeropuerto internacional de Bagdad, Irak, se llevó a cabo una operación para eliminar al Grl Qasem Soleimani, General de División iraní, comandante de la Fuerza Quds. Inicialmente según fuentes de inteligencia de los Estados Unidos de Norteamérica, la acción se iba a realizar mediante el uso de los helicópteros de ataque. Posteriormente se dio a conocer que la operación consistió en un ataque de precisión, con aviones no tripulados Reaper MQ-9.

La orden fue autorizada por el gobierno de Donald Trump. El objetivo de alto valor, estaba acusado de la muerte de cientos de ciudadanos y del ataque de una base militar estadounidense en Irak.

La operación consistió en una incursión mediante uso de aviones no tripulados, previa confirmación de que el blanco se encontraba saliendo del aeropuerto internacional con un convoy de dos vehículos, al momento que alcanzó una curva, el dron lanzó dos misiles que impactaron con precisión, eliminando el blanco.

Acá podemos evidenciar un esfuerzo por parte del área de inteligencia, en la búsqueda y confirmación del blanco seleccionado, como así también, el empleo de guerra electrónica para

interceptar comunicaciones del enemigo y ganar la superioridad electromagnética, como así también la operación de los drones a miles de kilómetros del objetivo.

Si bien aún nuestras Fuerzas Armadas no tienen desarrollado este sistema de armas, es factible contar con su incorporación, ya que su costo no es de gran consideración. Lo podemos ver en el desarrollo que hizo no hace mucho Turquía, Azerbaiyán y Siria en el empleo de esta tecnología, otorgando a la estructura de las Operaciones de Información otro elemento para poder satisfacer los efectos solicitados.

Queda expresamente comprobado la eficacia del uso de este tipo de sistema de armas, pudiendo así preservar el empleo de los grupos especiales para realizar operaciones que requieran la confirmación positiva del blanco en forma personal, valorizando y protegiendo de esta manera al personal que es un elemento de difícil reposición (BBC, 2021).

Conclusiones parciales

La Guerra de la Información ha ido creciendo geoméricamente desde mediados del Siglo XX hasta nuestros días por el incremento de nuevas tecnologías. En tiempos anteriores aun buscando los mismos objetivos, todo era más “artesanal” con mayor intervención de humanos. Se ejemplificó que la búsqueda de información sobre el terreno enemigo, condiciones meteorológicas, el velo y engaño, y demás operaciones similares, fueron utilizados por los estrategas y comandantes a través de la historia para buscar ventajas sobre el oponente con distintas denominaciones que las actuales, pero con la misma finalidad.

No obstante, habiéndose tratado en los últimos tiempos lo que se llama “Inteligencia de Señales” e “Inteligencia Humana”, el hombre, el factor humano que es el que finalmente programará, indicará donde buscar y qué y sobre todo decidirá, sigue siendo lo principal. Uno de los problemas, ya mencionado, es que la disponibilidad de tanta tecnología, sea para engañar, para reunir información, para localizar blancos, para individualizar blancos y personas, etc. va

llegando a un punto en que es tanta la cantidad de información que a veces resulta muy dificultoso completar el análisis humano antes de la decisión.

Ello requiere entonces de una organización estable y de alta coordinación y aptitud para el trabajo en equipo con una conducción centralizada.

En los ejemplos de las confrontaciones que hemos tratado, se pueden visualizar los avances técnicos antes referidos antes de los años, donde el dominio y el uso del espectro electromagnético, desde la 2da guerra mundial hasta Afganistán, se fue transformando en factor de éxito para emprender operaciones más eficientes a un menor costo pecuniario y humano.

Capítulo II: Plexo Normativo Nacional y Marco Doctrinario

“El arte supremo de la Guerra es someter al enemigo sin luchar.” (Sun Tzu, 544 a.c).

En este capítulo se analizará datos bibliográficos y la doctrina vigente en el propio IMT y en el de otros países en el marco regional y principales potencias mundiales, referido a la Guerra de la Información, como así también el ordenamiento legal argentino para determinar si nuestra normativa se ajusta a las exigencias requeridas.

Sección 1: Plexo Normativo Nacional

Es adecuado comenzar por las normas legales (Leyes) vigente en nuestro país para dar un apropiado y más oportuno marco al resto del análisis; para ello se han tomado las cuatro Leyes que tienen relación directa con el tema:

Ley 23.554 Ley de Defensa Nacional. Promulgada 26 abril 1988.

Ley 24.059 Ley de Seguridad Interior. Promulgada 06 enero 1992.

Ley 25.520 Ley de Inteligencia Nacional. Promulgada 03 diciembre de 2001.

Ley 27.126 Agencia Federal de Inteligencia. Promulgada 03 marzo 2015.

La Ley desde sus orígenes tiene su razón en la organización de la sociedad. Si el ser humano no viviera en comunidad quizás no fueran necesarias las leyes o normas para regular la vida en sociedad. Así entonces la Ley fue conformando un ordenamiento de derechos y de sanción a algunos comportamientos o su prohibición.

Los primeros ordenamientos jurídicos de los que se tiene conocimiento son de origen egipcio, posteriormente el conocido código de Hammurabi que data de varios miles de años antes de Cristo, Grecia carecía de códigos escritos, aunque aceptaba que la Ley se componía de lo divino - los dioses - los decretos o normas humanas y las costumbres. Estas fuentes eran interpretadas por los filósofos y militares.

Finalmente, así como Grecia fue la cuna de la filosofía y las formas del gobierno fue Roma quien dio con su derecho y el idioma latino verdadera formalidad a las leyes que se extienden hasta el presente.

Vimos que había fuentes divinas, humanas y costumbre. Traspolando eso a la actualidad podríamos decir que lo divino - aunque puede menospreciárselo con lo siguiente - podría ser la formación religiosa y moral de los legisladores, mientras que los decretos humanos responden a necesidades coyunturales y la costumbre a lo que es: manera de obrar de una persona, o colectividad que con el transcurso del tiempo o la repetición es adoptada y finalmente adquiere fuerza de precepto.

Las “Leyes de la Guerra”, recién incluidas en el derecho positivo luego de los Convenios de Ginebra en 1949, tuvieron su origen también en la costumbre. Vinieron a regularizarla ya que la mayoría de sus preceptos - con el tiempo - paulatinamente se iban normalizando y sólo se alteraban puntualmente por lo que de salvaje lleva la guerra en sí misma.

Pero hay también otras circunstancias acontecidas en nuestro país - y ya vamos llegando a nuestro punto - en que esas normas o leyes que quieren regular la vida en sociedad responden muchas veces a necesidades coyunturales, por ejemplo, la “Ley de Defensa de la Democracia”, de validez legal y legítima pero sobreabundante ante la Constitución y un sin número de costumbres.

Así entonces, en las últimas décadas y en relación a nuestro tema surgieron leyes que en algunos casos cubrían vacíos, pero también venían a atender asuntos y necesidades del momento.

Ley 23.554 de Defensa Nacional. Como en todas estas Leyes que trataremos brevemente debe tenerse en cuenta la fecha y las circunstancias históricas del momento en que fueron sancionadas y los tiempos anteriores y antecedentes de por sí inmodificables (InfoLeg, Defensa Nacional, 2021).

Esta Ley en lo que llaman “lo que el legislador quiso decir, o el espíritu” de la Ley viene a separar la intervención de las Fuerzas Armadas en cuestiones internas relativas a la seguridad; en tal sentido en su art. 2º indica que las FFAA están para disuadir o repeler agresiones de origen externo y en el art. 4º separa todo lo referido a seguridad interior como pertinente a otra legislación, veamos:

“art. 1º – La presente Ley establece las bases jurídicas, orgánicas y funcionales fundamentales para la preparación, ejecución y control de la Defensa Nacional.” (H.C.N. Ley N° 23.554)

art. 2º – La Defensa Nacional es la integración y la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieran el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva, para enfrentar las agresiones de origen externo.

Tiene por finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y la libertad de sus habitantes. (H.C.N. Ley N°23.554)

Y entrando en asuntos relativos a Información e Inteligencia el art.15º dice:

El organismo de mayor nivel de inteligencia proporcionará la información e inteligencia necesarias a nivel de la estrategia nacional de defensa. La producción de inteligencia del nivel Estratégico Militar estará a cargo del organismo de inteligencia que se integrará con los organismos de inteligencia de las Fuerzas Armadas y que dependerá directamente del Ministro de Defensa. Las cuestiones políticas no podrán constituir en ningún caso hipótesis de trabajo de organismos de inteligencia militar. (H.C.N. Ley N°23.554).

Finalmente, en el Título VIII Disposiciones Transitorias en el art. 45º establece que el Consejo de Defensa Nacional deberá en un plazo de 365 días elaborar anteproyectos de ley

mínimos que se citan seguidamente en el art.46º, siendo de interés el inciso e) que dice “Ley sobre el Sistema Nacional de Inteligencia, que contemple el control parlamentario”.

Es dable recordar el concepto de “agresión”, normado internacionalmente mediante Resolución de la Asamblea General de las Naciones Unidas N° 3314(XXIX) de fecha 14 de diciembre de 1974:

La agresión es el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de las Naciones Unidas, tal como se enuncia en la presente definición. (Crimen de agresión, 2021).

Esta Ley, vino en su esencia a separar el ámbito de empleo de las FFAA encuadrándolo exclusivamente en las agresiones de origen externo, su sanción tuvo relación con la llamada “Doctrina de Seguridad Nacional” o Interna, por la cual las FFAA podían intervenir - sobrepasadas las fuerzas policiales y de seguridad - en asuntos internos.

Respondía a un período de transición en el cual ya agonizaba una agotada postura de las FFAA cuál era su intervención en la política, postura hoy inexistente.

En nada limita el empleo de las Operaciones de Información durante y después del conflicto, pero queda claro que la Guerra de la Información se emplea antes durante y después del conflicto. Ese “antes” en un ambiente de la Guerra de la Información se realizan Operaciones de Información para crear una valiosa ventaja sobre el oponente, de la misma forma, éste hará lo propio. Pero hasta el momento no está normado dicho empleo, dejando así un vacío legal y por ende doctrinario.

La solución de esta situación es necesario clarificarla para no caer en el error, en caso de su empleo, de pasar a ser el agresor en vez del agredido, siendo que como vimos, la definición de agresión dada por la Asamblea General de las Naciones Unidas, no contempla una invasión

incruenta a través del ciberespacio a nuestro territorio soberano para los fines de guerra que buscarán obtener otros Estados.

Ley 24.059 de Seguridad Interior. Pasados tres años y nueve meses y quinientas cinco leyes desde la anterior se sanciona la Ley de Seguridad Interior que viene también a poner límites al empleo de las Fuerzas, cuestión clara que no implica juicios (InfoLeg, Seguridad Interior, 2021).

Los aspectos más importantes que pueden tenerse en cuenta para este trabajo son los siguientes:

En su art. 1º “La presente Ley establece las bases jurídicas, orgánicas y funcionales del sistema de planificación, coordinación, control y apoyo del esfuerzo nacional de policía tendiente a garantizar la seguridad interior”.

art.7º “El Ministro de Defensa forma parte del Sistema de Seguridad Interior”.

art.27º En particular el Ministerio de Defensa dispondrá en caso de requerimiento del Comité de Crisis que las FFAA apoyen las operaciones de seguridad interior mediante la afectación a solicitud del mismo, de sus servicios de arsenales, sanidad, veterinaria, construcciones y transporte, así como elementos de ingenieros y comunicaciones para lo cual se contará en forma permanente con un representante del Estado Mayor Conjunto en el Centro de Planeamiento y Control de la Subsecretaría de Seguridad Interior.

art 28º “Todo atentado en tiempo de paz a la Jurisdicción Militar independientemente de poner en forma primordial en peligro la aptitud defensiva de la nación, constituye asimismo una violación a la seguridad interior.”

art.29º “En los casos previstos en el art. 28º constituye una obligación primaria de la autoridad militar la preservación de la Fuerza Armada y el restablecimiento del orden dentro de la aludida jurisdicción, de conformidad con las disposiciones legales vigentes en la materia.

art. 31° Sin perjuicio del apoyo establecido en el art. 27°, las FFAA serán empleadas en el restablecimiento de la seguridad interior dentro del territorio nacional en aquellos casos excepcionales en que el sistema de seguridad interior descrito en esta ley resulte insuficiente a criterio del Presidente de la Nación para el cumplimiento de los objetivos establecidos en el art.2° (...) resguardo de la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías, las instituciones(...))

art.32° “(...)el Presidente (...) dispondrá el empleo *de elementos de combate* de las FFAA para el restablecimiento de la normal situación de seguridad interior, previa declaración del estado de sitio.”

art.32° inc. c) “Tratándose lo anterior de excepcional empleo, que sería desarrollado en casos de extrema gravedad la misma no incidirá en la doctrina, organización, equipamiento y capacitación de las FFAA, las que mantendrán las características de la aplicación de la Ley 23.544.”

Para comenzar, se puede afirmar que esta Ley en general, tampoco pone límites a la Guerra de la Información en su letra contra una agresión externa, pero si a la hora de contemplar un excepcional empleo interno de acuerdo al art 32.

Vuelve a poner los límites geográficos y sociales de actuación. Dice claramente quien se ocupa de lo “interior”.

La Ley - no debe ser detallada pero sí clara en su “espíritu” - Volviendo a los artículos 31° y 32°, quedan preguntas o vacíos sin respuestas del legislador: Si las FFAA siguen organizadas equipadas y entrenadas para el conflicto externo, ¿cómo enfrentarán uno interno? Concretamente, el art. 32° inc c), pone límites a un posible desarrollo organizativo, doctrinario de equipamientos, del IMT; si se apreciase eventualmente la necesidad de planificar esta hipótesis de conflicto, donde la Guerra de la Información tendría un rol importante, al expresar: “(...) tratándose lo anterior de excepcional empleo, que sería desarrollado en casos de extrema

gravedad la misma no incidirá en la doctrina, organización, equipamiento y capacitación de las FFAA, las que mantendrán las características de la aplicación de la Ley 23.544.”, ya que como se verá más adelante, el IMT en cuanto a la Guerra de la Información, debería crear organizaciones, reforzar el equipamiento, redactar doctrina específica y capacitar a los operadores, para poder intervenir en ese ambiente particular en el marco externo, pero hasta aquí no habría problemas, ya que sería una evolución organizativa propia de la modernización de sus sistemas, pero ante un eventual empleo en el marco interno, necesariamente deberá adaptar su doctrina, organización y capacitación para esa delicada y controvertida misión.

Ley 25.520 de Inteligencia Nacional. Mil cuatrocientas sesenta y una leyes después vienen a sancionarse esta Ley de Inteligencia Nacional que es la que más se acerca al tema en desarrollo, pero no es prescindente de las anteriores (InfoLeg, Ley de Inteligencia Nacional, 2021). Sus aspectos más importantes en relación la inteligencia e información militar son los que siguen:

art. 2° A los fines de la presente ley y de las actividades reguladas por la misma. Se entenderá por:

inc. 4) Inteligencia Estratégica Militar a la parte de la Inteligencia referida al conocimiento de las capacidades y debilidades del potencial militar de los países que interesen desde el punto de vista de la Defensa Nacional, así como el ambiente geográfico de las áreas estratégicas operacionales determinadas por el planeamiento Estratégico Militar.

art. 6° “Son organismos del Sistema de Inteligencia Nacional:

(...) 3. La Dirección Nacional de Inteligencia Estratégica Militar”

art. 10° Créase la Dirección Nacional de Inteligencia Estratégica Militar dependiente del Ministro de Defensa, de conformidad con lo establecido en el Artículo 15 de la Ley 23.554.

Tendrá como función la producción de Inteligencia Estratégica Militar.

Los organismos de inteligencia de las Fuerzas Armadas tendrán a su cargo la producción de la Inteligencia Estratégica Operacional y la Inteligencia Táctica necesarias para el planeamiento y conducción de operaciones militares y de la Inteligencia Técnica Específica.

art. 11° Queda prohibida la creación conformación y funcionamiento de asociaciones, instituciones, redes y grupos de personas físicas o jurídicas que planifiquen y/o ejecuten funciones y actividades de inteligencia en cualquiera de sus etapas asignadas por la presente ley a los organismos integrantes del Sistema de Inteligencia Nacional.

art.13° Conforme los lineamientos y objetivos establecidos por el Presidente de la Nación, la Secretaría de Inteligencia tendrá las siguientes funciones:

(...) inc. 11: Proporcionar al Ministerio de Defensa la información e inteligencia que fuere menester para contribuir en la producción de la Inteligencia Estratégica Militar, de conformidad a lo estipulado sobre la materia en el artículo 15 de la ley 23.554.

Tampoco esta Ley restringe la Guerra de la Información, en cierto modo la facilita en la letra de su art. 2° en función de que al definir la Inteligencia Estratégica Militar describe las tareas que puede hacer para cumplir con su misión, y precisamente, son las que la Guerra de la Información, en parte, necesita para su planeamiento y empleo en cuanto al conocimiento de las capacidades y debilidades del posible oponente como así también el ambiente geográfico de interés.

Ley 27.126 Agencia Federal de Inteligencia (AFI). Mil seiscientos seis leyes después, en marzo de 2015, se promulga la ley llamada AFI, de su texto podemos tomar como de interés los siguientes puntos que (InfoLeg, Agencia Federal de Inteligencia, 2021), como en muchos casos de esta Ley modifican los artículos de la Ley N° 25.520 de Inteligencia Nacional:

art.2° Sustitúyase el inciso 1 del artículo 2° de la ley 25.520, por el siguiente texto:

1. Inteligencia Nacional a la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la Seguridad Interior de la Nación.

art. 3 Sustitúyase el inciso 1 del artículo 4° de la ley 25.520, por el siguiente texto:

Ningún organismo de inteligencia podrá:

1. Realizar tareas represivas, poseer facultades compulsivas, cumplir, por sí, funciones policiales. Tampoco podrán cumplir funciones de investigación criminal, salvo ante requerimiento específico y fundado realizado por autoridad judicial competente en el marco de una causa concreta sometida a su jurisdicción, o que se encuentre, para ello, autorizado por ley, en cuyo caso le serán aplicables las reglas procesales correspondientes.

art. 6°: Sustitúyase el artículo 8° de la ley 25.520 por el siguiente texto:

art. 8°: Las funciones de la Agencia Federal de Inteligencia serán las siguientes:

1. La producción de inteligencia nacional mediante la obtención, reunión y análisis de la información referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior, a través de los organismos que forman parte del Sistema de Inteligencia Nacional.

2. (...).

La ley al igual que las otras vistas, no afecta en lo que a Guerra de la Información se refiere, y las consideraciones son similares a las expuestas en las conclusiones de la ley 25.520.

Comentarios finales respecto al marco legislativo vigente

El marco legislativo vigente, en general, “en su letra” en nada afecta al eventual empleo de la Guerra de la Información en caso de una agresión de origen externo.

La ley 25.520 Ley de Inteligencia Nacional, habilita a la Inteligencia Estratégica Militar, a la Operacional, y a la Táctica a realizar esfuerzos para el conocimiento de las capacidades y debilidades del potencial militar de los países que interesen desde el punto de vista de la Defensa Nacional, así como el ambiente geográfico de las áreas estratégicas operacionales determinadas por el planeamiento Estratégico Militar. En consecuencia, la información e inteligencia básica que es necesaria dominar para el correcto y oportuno empleo de las operaciones constitutivas de la Guerra de la Información está normada en nuestra legislación. Las limitaciones que se imponen en general, están referidas al empleo de las FFAA en el marco interno, no obstante, la Ley 24.059 de Seguridad Interior en su art.34, habilita al Presidente de la Nación al empleo de elementos de combate de las FFAA en forma excepcional para restablecer la normal situación de seguridad interior, pero sin que esta imposición, incida en la doctrina, organización, equipamiento y capacitación de las FFAA

Esta última imposición normativa, afecta directamente a los elementos de combate y de la misma manera al elemento a crear para operar en un ambiente de la Guerra de la Información, ya que el empleo de las FFAA en el marco interno necesariamente debería hacer variar el concepto de empleo, organización, equipamiento, y adiestramiento, en función de que cambiaría la naturaleza del conflicto.

Asimismo, queda un vacío normativo en cuanto al concepto de empleo de las Operaciones de Información antes del conflicto a modo de disuasión y “Alerta Temprana Estratégica” (DPDN, 2021), y especialmente para la protección el sistema propio de Comando, Control, Comunicaciones, Informática, Inteligencia, (C3I2) y afectación al del oponente.

La creación de la Subsecretaría de Ciberdefensa como órgano dependiente del Ministerio de Defensa y del Comando Conjunto de Ciberdefensa en el ámbito del Estado Mayor Conjunto de las Fuerzas Armadas, auguran un avance concreto, en cuanto a normativas, equipamiento y capacitación de los recursos humanos para intervenir en el ámbito de la Guerra de la Información.

Sección 2: Doctrina Propia del Instrumento Militar Terrestre

Luego del análisis del marco legal, amerita concentrarnos en la doctrina militar vigente en nuestro país, a fin de completar lo propuesto en este capítulo.

En el reglamento ROB 00-01 Conducción de la Fuerzas Terrestres, es el único donde se menciona la Guerra de la Información. En el art. 2009 Inteligencia. se la describe parcialmente:

La inteligencia sustenta, esencialmente, su función en la obtención y procesamiento de la información obtenida. Es por ello que tanto las propias Fuerzas como las del enemigo, en la búsqueda del conocimiento de los distintos factores que intervienen en una situación táctica, darán origen a la denominada Guerra de la Información, llevándola a cabo en el apoyo de sus respectivas Fuerzas en la ejecución de las distintas operaciones militares”, para luego pasar a definirla como:

Guerra de la Información es el uso y manejo de la información con el objetivo de conseguir una ventaja decisiva sobre el enemigo, pudiendo abarcar tanto la obtención de información táctica y la confirmación de su veracidad, como la desinformación, a efectos de afectar las operaciones del enemigo, socavando la calidad de información obtenida por este y negándole la oportunidad de búsqueda y reunión de información” (Ejército Argentino, Conducción para las Fuerzas Terrestres (ROB - 00 - 01), 2015, pág. 8).

Por otro lado, cuando este reglamento se ocupa de las Operaciones Complementarias en su Cap VII, deja sentado en sus arts. 7056, 7060 y 7100 que tanto la Guerra Electrónica, la

Comunicación Social Aplicativa al Combate (COSACO) y la Ciberdefensa, integran el conjunto de las operaciones que conforman la Guerra de la Información.

Pero existe un vacío doctrinario en cuanto a su organización, equipamiento, composición, y empleo. Solo se la menciona y define. La doctrina disponible del área de Inteligencia y la doctrina de la Comunicación Social Aplicativa al Combate(COSACO) no están articuladas entre si y al momento de escribir esta investigación la doctrina de Ciberdefensa no está completamente desarrollada, por lo tanto, podemos aseverar que no existe una doctrina en el IMT referida en especial a la Guerra de la Información. es más, no se mencionan en el reglamento base del IMT cuales otras operaciones, además de las cuatro enumeradas, deberían formar parte de una organización que esté en capacidad de operar en un ambiente de Guerra de la Información.

Así las cosas, podemos concluir que no se dispone de una doctrina particular que se ocupe de la Guerra de la Información. Existen reglamentos que, en forma independiente, norman, los procedimientos de empleo de Inteligencia y COSACO, que son dos de las operaciones que se emplean en ese tipo de ambiente operacional, pero no están articulados entre sí para operar coordinadamente, y no está totalmente desarrollada la doctrina de Ciberdefensa que es otra de las operaciones que la integran, dejando sin aclarar, cuales otras deberían integrarlas.

No se advierten contradicciones entre la normativa legal y lo que determinan las normativas reglamentarias militares, pero es dable advertir, que la concordancia entre la legalidad y las operaciones se da no sólo en la letra y en la interpretación sino también en la confianza mutua entre el factor político que dicta las normas legales y el factor militar que ejecuta la preparación y la guerra. Ciñéndonos a la Guerra de la Información veamos lo que ocurrió en el ejemplo de la Guerra del Golfo del Capítulo I: luego de una campaña anunciada a todo el mundo la lucha armado no sobrepasó las dos semanas; al poco tiempo después

comenzaron a circular fotografías de maltratos a soldados iraquíes por parte de soldados de la coalición. ¿Qué hizo la coalición ante esos hechos que eran innegables? Una intensa campaña de guerra psicológica como parte de la Guerra de la Información para proteger a sus tropas, al margen de las medidas disciplinarias que se hubieran podido o no haber adoptado.

Sección 3: Doctrina de potencias mundiales

Estados Unidos de Norte América. Aún con las críticas acerca de cierta debilidad ante la retirada de Afganistán los Estados Unidos siguen siendo la mayor potencia de Occidente y también mundial, ya que China y la Federación Rusa sin desmerecerlas son potencias que están en la competición, pero no han llegado aún a sobrepasar al potencial norteamericano.

Yendo al tema que nos ocupa, la Guerra de la Información en los EEUU es tan vigente como activa, abarcando periódicamente acciones de todo el ciclo de inteligencia que conocemos además de operaciones abiertas o encubiertas. Su actividad es permanente desde hace ya varias décadas.

Su mayor esfuerzo financiero militar, estaría volcado a este campo el de la información. Ha llegado a un punto tal de perfeccionamiento en los últimos treinta años que a la fecha se puede inferir sin temor a equivocarse que en este campo de acción son los más avanzados en tecnología.

En los años noventa la llamaban inteligencia de señales e inteligencia humana. El problema que entonces se planteaban en EEUU se reducía a dos cosas:

La imposibilidad de procesar el volumen de información reunida.

El no alcanzar a comprender aún la idiosincrasia de sus enemigos terroristas.

Subsidiariamente persistía cierto celo entre las llamadas agencia relativas a Inteligencia en lo referido a compartir información en forma fluida y constante, coordinar operaciones, etc.

Con el tiempo y sobre todo a partir de los sucesos del 11S (Cuatro ataques con aviones el 11 de septiembre del 2001) fueron allanando los inconvenientes mencionados.

Lo particular de los Estados Unidos es que su compleja pero dinámica Guerra de la Información tiene como blanco o ámbito no sólo al enemigo a enfrentar sino a la opinión pública propia interna y mundial; a tal punto ha llegado que aun pasando del silencio a llenar de información apreciaciones, lista de blancos, desinformar y bloquear todo lo pertinente del enemigo, llena o no las tapas de los diarios de considerarlo necesario. ¿Y cómo lo logra? No sólo por la tecnología, sino por la Unidad Nacional ante situaciones de agresión o peligro.

Toda orientación o intención parte desde las jerarquías más altas de Estados Unidos, se sostiene en su Constitución Nacional. Queda claro, sin que este explícitamente indicado en su letra, que tiene definido dos objetivos cortos, pero llenos de:

- Asegurar la vida y la libertad de todo estadounidense en cualquier lugar del mundo.
- Crear un orden económico mundial favorable y estar dispuesto a defenderlo.

Entre muchas otras, podemos citar a modo de ejemplo, las siguientes doctrinas desarrolladas por la doctrina por las Fuerzas Armadas de los Estados Unidos de Norte América:

- Joint Operations (USA Joint Chiefs of Staff, Joint Operations (JP 30-0 17), 2017).
- Joint Doctrine for Information Operations (USA Joint Chiefs of Staff, Joint Doctrine for Information Operations (USA JOINT PUP 3-13), 1988).
- Information Operations. (USA Joint Chiefs of Staff, Information Operations (JP 3-13), 2012).
- Joint Operation Planning. (USA Joint Chiefs of Staff, Joint Operation Planning (JP 5-0), 2011).

Federación Rusa. “La información se ha convertido en un arma destructiva como una bayoneta, una bala o un proyectil.” (Vladimir Slipchenko,s.f.)

El Ejército de los Estados Unidos de Norteamérica, considera que el desarrollo de competencia son acciones que perduran en un determinado tiempo, aprovechando las condiciones del ambiente operacional para tener relativa ventaja, sin alcanzar una situación de un conflicto armado. La importancia del desarrollo de esta capacidad es crear un punto muerto

estratégico y operacional que posibilite una adecuada libertad de acción en cualquier dominio que se plante. Esto se logra mediante la relación de las distintas acciones políticas, económicas, guerra no convencional, Guerra de la Información y empleo de sus fuerzas de propósito general.

Rusia en particular utiliza su poder relativo para influir sobre este dominio a través de la fracturación de alianzas, asociaciones y acuerdos, principalmente utilizando en forma eficiente el empleo de la información buscando lograr de esta manera el debilitamiento de las relaciones de sus aliados.

Estas acciones que surgen de manera planificada y armónicamente coordinadas, suelen confundir hasta los mismos militares por la delgada línea que existe entre los diferentes dominios, sumado a los nuevos escenarios bélicos donde conviven aspectos de la sociedad, del gobierno y hasta aspectos de redes extralegales.

La doctrina oficial de las Fuerzas Armadas Rusas, establecen que solo tomarán medidas militares cuando se agoten todas las acciones políticas, económicas, diplomáticas, jurídicas, informativas y todas aquellas acciones no violentas, protegiendo de esta manera los intereses vitales de los rusos, la sociedad y el Estado. Por esto, hay una tendencia de trasladar los riesgos y lo posibles conflictos al espacio de la Información, siendo que esta última ha sido desarrollada con mucho énfasis por la ciencia militar durante décadas.

Dicha actividad es tan importante que la equipara con la política nacional. Posee en los componentes de Guerra de Información del Estado Mayor General, la más variada configuración imaginativa. Dentro de su visión holística de este dominio informacional, a grandes rasgos podemos nombrar, organización de derechos humanos, bases militares en el extranjero, industrias de computadoras y películas, empresas de militares privadas, hasta la necesidad de contar con académicos que obtuvieron el premio Nobel. Todos los esfuerzos están dirigidos a proteger y contrarrestar los ataques recibidos contra la Federación Rusa.

Este dominio está dividido en: Informativa Técnica, que incluye ciberataques y guerra electrónica e Informativa Psicológica, que consiste en una gran gama de crear imprevisibilidad. Los conjuntos de estas operaciones tienen como finalidad que el enemigo se auto-desorganice y se auto-desoriente.

También es importante remarcar que su doctrina está en constante revisión. Están volviendo a conceptos de su Ejército Rojo, como el concepto de propaganda o contra propaganda, otro término de antaño como sabotaje que incluyen a las Operaciones de Información referidos al engaño, desviación y desorientación. También surgen términos como de desorganización y fragmentación que buscan afectar la toma de decisiones y la conducción en los momentos críticos. Todos estos conceptos tienen como finalidad alterar la naturaleza del combate.

Así como hay un revisión doctrinaria y definición del alcance de este tipo de operaciones, en forma simultanea se suma la tecnología, que permite potenciar estas competencias mencionadas en los párrafos anteriores.

A modo de ejemplo podemos mencionar sistemas de vehículos de combate que tendrán capacidades casi humanas que estarán en condiciones de poder realizar una evaluación del entorno, seleccionar los mejores modos de acción, comunicarse y decidir sin la intervención de un operador (Wilhelm, Tom, 2021).

Desde la visión del Grl Valeri Vasilevich Guerásimov, actual jefe el Estado Mayor de las Fuerzas Armadas y de Ruslán Tsálikov Primer Vice Ministro de Defensa, la guerra total coloca a la política y la guerra en la misma esfera de acción. En esta categoría se concentran enfoques técnicos, tácticos y estratégicos tales como:

- Creación de movimientos rebeldes.
- Revolución de color.
- Cyberwar/ciberguerra.

- Hacktivism.
- Guerra de la Información
- Interferencia operativa (dentro de otros países, Operaciones psicológicas)
- Medidas proactivas (Maskirovka) desinformación e información.
- Guerra centrada en redes (Guerra en red).
- Operaciones financieras Operaciones de alto nivel.
- Armas tecnológicas (ataques aéreos rusos sobre Siria).
- La Guerra de la Información y las noticias falsas tienen un valor especial y "futurista"

para Guerásimov, y son comparables al uso masivo de la fuerza militar.

Las redes sociales y los medios de comunicación son una plataforma propicia para inyectar mensajes falsos en los canales de comunicación de la oposición, realizar actividades de desinformación y filtrar informaciones falsas, verdaderas o medias verdades (entre las cuales se recuerda "el falso ataque químico de las fuerzas de Bashar Al Assad contra la población de la Duma ").

El uso de alta tecnología y herramientas para guerras de media y alta intensidad como la ciberguerra, y la estructuración de mecanismos de ataque centrado en redes para guerras de baja intensidad como en el caso de Netwar, adquiere un relevante importancia de acuerdo con la doctrina Guerásimov, para lo cual el Estado Mayor ruso puso énfasis en la creación de divisiones encargadas de la Guerra Cibernética y las Operaciones de Información, para alcanzar de esta manera, los objetivos, políticos, estratégicos y tácticos, utilizando un mínimo esfuerzo militar y el empleo de las Nuevas Tecnologías de la Información y las Comunicaciones (NTIC's) (Tepedino, Sebastián, 2021).

Otro aspecto a mencionar es que, en los conflictos modernos actuales, la información se ha convertido en algo tan relevante como los efectos tácticos a la hora de determinar el resultado de las operaciones, en la actualidad, los elementos tácticos tienen una capacidad

reducida para vislumbrar o incidir en el Ambiente Informacional (AI). En principio, es de suponer, que las Operaciones de Información se ejecutan solamente en el nivel operacional y estratégico, sin embargo, este concepto está siendo cuestionado dado el actual ambiente operacional, donde los elementos tácticos se ven influenciado por este tipo de operaciones y necesitan desarrollar la capacidad de entender y repeler las acciones. De lo contrario el enemigo seguirá estableciendo los escenarios y el desarrollo de las nuevas capacidades (Derleth, 2021).

Podemos decir que Rusia al igual que China, tienen el mismo criterio - en general - que los Estados Unidos en cuanto al empleo de las FFAA, su desarrollo, su capacitación, etc. Disponen también de sistemas para actuar en un ambiente de la Guerra de la Información modernos y actualizados. La disuasión entre ellos y los Estados Unidos sigue siendo el mejor salvavidas para el mundo.

“Las diferencias en los niveles estratégico, operacional y táctico, así como entre las operaciones ofensivas y defensivas, están desapareciendo.” (General Valery Guerásimov, 2021).

República Popular China. Las fuerzas armadas chinas desde antaño han mantenido estructuras tácticas operativas y doctrinas militares rígidas. Con el advenimiento de las NTIC's y el uso del ciberespacio con fines militares, ha incursionado en la Guerra de la Información.

China desde hace 25 años ha comenzado con el cambio sustancial de su doctrina estrategias, composición y organización militar poniendo énfasis inicialmente al armamento cinético convencional, incorporando luego el desarrollo del uso del ciberespacio para el uso de fines militares. Su objetivo en este campo es convertirse en un líder en la tecnología de la información y la comunicación.

A la luz de los avances en materia militar de los EEUU observados en la Guerra del Golfo, comenzó a desarrollar su doctrina sobre la Guerra de la Información basada en la de EEUU y Rusia.

A partir de 1997 a la fecha, realizó cientos de ejercicios militares sobre esta materia, especulando que los objetivos de la simulación eran afectar a través del ciberespacio a Taiwán, Japón, y Corea del Sur, sin perder de vista que el objetivo principal es neutralizar a ejércitos con tecnología de punta (EEUU y otros países occidentales).

El esfuerzo en lo que respecta a Guerra de la Información, está dirigido a la detección de las fuentes de información del oponente, canales de información, procesadores de información y sistemas de toma de decisiones, logrando con ello, superioridad en la información, ruptura e interrupción del control de las capacidades informacionales, y mantener los sistemas y capacidades propios. Todas estas acciones, integradas con tácticas de Guerra Electrónica, Operaciones Psicológicas y Guerra Legal, entre otras.

La Guerra de la Información, China la concibe como complemento a los ataques cinéticos, a los efectos de lograr sus objetivos con golpes contundentes, rápidos y difíciles de responder por parte del adversario.

Wang Xusheng, Su Jinhai y Zhang Hong, autores de la Academia de Tecnología Electrónica del Ejército de Liberación Popular (ELP), enlistan los elementos esenciales de la teoría de la Guerra de la Información:

- La primera meta es atacar los sistemas de control y comando.
- Pelear con rapidez para que el enemigo no conozca el estado actual del campo de batalla en donde se encuentre.
- Atacar las autoridades de comando, personal del cuartel general y la sede del cuartel general.
- Proyectar escenarios con mayores roles para fuerzas flexibles.
- Destruir los “ojos y oídos” del enemigo, protegiendo los sistemas amigables.
- Usar sistemas de redes multinodal/flujo/frecuencia equipados con información engañosa y procedimientos ocultos para asegurar la seguridad.

- Usar equipos digitalizados.

El objetivo de China para la guerra, es una combinación rápida y contundente de un ataque cibernético en primer lugar, seguido por un ataque cinético que dejase pocas posibilidades al oponente de represalias cibernéticas y cinéticas.

El ELP, cuenta con dos departamentos encargados de las medidas ofensivas y defensivas para el uso del ciberespacio: el primero se ocupa de la coordinación de todas las operaciones cibernéticas que realicen espionaje, vigilancia, y reunión de información tanto en otros países como en el propio y el otro departamento es responsable de las contramedidas y ataques a las redes en caso de una guerra electrónica (Ángeles, Ernesto, 2021).

Sección 4: Doctrina en el Marco Regional.

Una vez mencionado el marco mundial a través de las principales potencias mundiales, es preciso realizar una revisión de la doctrina de los países de la región (Chile y Brasil) para poder determinar en qué situación relativa nos encontramos, para estar a la altura de las exigencias que nos impone el campo de combate moderno. Es válido aclarar que la necesidad de nivelar esta ventaja operacional, es un factor determinante al visualizar la campaña, siendo una herramienta más que cuenta el comandante dentro de su diseño operacional.

Es por eso que a continuación realizaremos un cuadro comparativo con la doctrina que actualmente utilizan los países de interés del marco regional.

Cuadro 1. Comparación entre la Doctrina del Ejército de Chile y del Ejército de Brasil.

PARÁMETRO	Ejército de Chile (RDO – 20909- Operaciones de Información, 2010)	Ejército de Brasil (EB20-MC-10.213- Operaciones de Información, 2014)
Nivel de la conducción	Estratégico Militar, Operacional	Estratégico Militar, Operacional

PARÁMETRO	Ejército de Chile (RDO – 20909- Operaciones de Información, 2010)		Ejército de Brasil (EB20-MC-10.213- Operaciones de Información, 2014)
Finalidad	Afectar la toma de decisiones sobre el adversario influyendo sobre su capacidad para explotar y proteger la información, sistema de mando y control y los sistemas de telecomunicaciones, mientras se protegen los propios,		Hace referencia que no solo el conflicto es sobre Estados, sino que actualmente hay una mayor preponderancia a entornos donde reina la incertidumbre, y es más difícil identificar al enemigo ya sea estatal o no, regular o irregular.
Relación de dependencia	Dependerá de la función de operaciones y estrecha relación con la función de inteligencia.		Si bien taxativamente no menciona el área que lleva adelante las actividades podemos inferir que es el área de operaciones, con vinculación directa con el área de inteligencia.
Operaciones que la conforman	Ofensivas	<ul style="list-style-type: none"> -La Decepción -Operaciones Psicológicas. -Ataques a Redes 	De las Operaciones se destacan: Comunicación Social, operaciones de apoyo a la información, Guerra electrónica, guerra cibernética e inteligencia
	Defensivas	<ul style="list-style-type: none"> -Seguridad en las Operaciones -Acciones de decepción 	

PARÁMETRO	Ejército de Chile (RDO – 20909- Operaciones de Información, 2010)	Ejército de Brasil (EB20-MC-10.213- Operaciones de Información, 2014)
	<ul style="list-style-type: none"> -La propaganda del adversario. -La contrainteligencia -Guerra Electrónica 	
	Operaciones de asuntos civiles	
Definición	Conjunto de acciones coordinadas que se realizan para influir en la toma de decisiones de un adversario en apoyo de la consecución de los objetivos propios, influyendo en su capacidad para explotar y proteger la información, en los sistemas de mando y control, mientras se resguardan los propios,	Consisten en actuar metodológicamente capacidades integradas relacionadas con la información, junto con otros vectores, informar e influir en grupos e individuos, así como afectar el ciclo de toma de decisiones del oponente, mientras protegemos a los nuestros. Además tienen como objetivo evitar, prevenir o neutralizar los efectos de acciones adversas en la dimensión informativa
Dimensión donde actúa	<ul style="list-style-type: none"> -Dimensión Física -Dimensión Informativa -Dimensión Cognitiva 	<ul style="list-style-type: none"> -Dimensión Humana -Dimensión Informacional.

PARÁMETRO	Ejército de Chile (RDO – 20909- Operaciones de Información, 2010)	Ejército de Brasil (EB20-MC-10.213- Operaciones de Información, 2014)
		-Dimensión Física (Perspectiva Cognitivo, Físico y logística)
Principios	<ul style="list-style-type: none"> -Dirección del mando y su ampliación personal. -Coordinación estrecha. -información e inteligencia precisa. -Planificación centralizada y ejecución descentralizada. -Planificación basado en Efectos. -Implicación temprana y preparación oportuna. -Análisis y seguimiento de los efectos. 	<ul style="list-style-type: none"> -Dirección e implicación directa del comandante. -Estricta coordinación -Actividad de Inteligencia precisa. -Planeamiento centralizado y ejecución descentralizada. -Planeamiento basada en Efectos. -Envolvimiento previos y preparación anticipada. -Análisis y acompañamientos de los efectos
Tipo de Estructura	Tipo Célular (se designa un asesor de INFOOPS bajo supervisión directa de operaciones E3	Tipo Célular
Integrantes De la Célula	<ul style="list-style-type: none"> -Oficial de Seguridad de operaciones. -Oficial de guerra electrónica -Oficial de Decepción 	<ul style="list-style-type: none"> -Sección operaciones -Secciones de Inteligencia -Sección planeamiento. -Sección comunicación social

PARÁMETRO	Ejército de Chile (RDO – 20909- Operaciones de Información, 2010)	Ejército de Brasil (EB20-MC-10.213- Operaciones de Información, 2014)
	-Oficial de operaciones Psicológicas. -Oficial de destrucción física. -Oficial de información pública. -Oficial cooperación cívico militar. -Oficial de sistema de telecomunicaciones y operaciones en redes de sistema de información.	-Sección operaciones de información -Sección Asuntos civiles. -Guerra cibernética. -Geo información -Guerra electrónica. -Seguridad en las operaciones. -Operaciones de apoyo e información. (Normalmente jefe de la Célula) – CRI (capacidades relacionadas a la información) -Oficial de Decepción. -Elementos de apoyo de fuego. -Fuerzas especiales. -Comunicación Social

Fuente: (RDO – 20909- Operaciones de Información, 2010; EB20-MC-10.213- Operaciones de Información, 2014).

Si bien ambos reglamentos toman como base la doctrina norteamericana, podemos encontrar ciertas diferencias y similitudes en la conformación de las células para operar, como así también en la definición del concepto Operaciones de Información.

La principal similitud que tiene ambos ejércitos sobre este tipo de operaciones, es como afectar la toma de decisiones del oponente y proteger la propia. Una herramienta que puede ser

utilizada por todos los integrantes que conforman esta organización como así también el órgano de dirección, es el ciclo de Observación, Orientación, Decisión y Acción (OODA). Este concepto fue desarrollado por el Coronel John Boyd, ex piloto de combate de la Fuerza Aérea de EEUU (USAF), obtenida luego de un intenso combate aéreo durante la II Guerra Mundial.

Básicamente esta teoría consiste en reducir el proceso de toma de decisiones antes, durante y después de los combates. La repetición y el uso permanente de éste ciclo posibilita al decisor obrar en forma anticipada, eventualmente saltando algún paso, pero como objetivo final busca adelantarse en el proceso de toma de decisiones del enemigo, logrando de esta manera parálisis por análisis por parte de quien recibe el efecto, dando una ventaja significativa al que lo realice en tiempo y forma. Es por eso que se remarca la importancia de internalizar esta opción de razonamiento que según Boyd, aquel contendiente que consiguiese cerrar el ciclo con mayor velocidad y precisión obtendrá una marcada ventaja (Spretz, Norberto Ivan, 2018).

Es por eso que podemos decir, cuando le preguntaron a John Boyd qué había hecho para derribar cinco aviones en un día de combate dijo: "Simple, cuatro de ellos nunca supieron que yo estaba en su mismo cielo".

Conclusiones parciales

Los principales ejércitos regionales, tienen desarrollada la doctrina del tema que nos ocupa mediante reglamentos llamados "Operaciones de Información", cada uno con su identificación interna particular, lo que nos deja en clara desventaja doctrinaria para operar en este tipo de ambiente.

Si bien ambos reglamentos toman como base la doctrina norteamericana, podemos encontrar ciertas diferencias y similitudes en la conformación de la Células para operar, como así también en la definición del concepto Operaciones de Información.

Ambos hacen depender las actividades a desarrollar del área de Operaciones, con una clara influencia del área de Inteligencia

Las operaciones a desarrollar son similares en su contenido, aunque no con idéntica denominación, salvo Guerra Electrónica común a ambos ejércitos. El reglamento brasilero, enumera operaciones que pueden contener varias acciones del reglamento chileno, por ejemplo, Guerra Cibernética, al englobar el ciberespacio como campo de operaciones, puede contener en su concepto el empleo de operaciones de Decepción, Operaciones Psicológicas, Propaganda, Contra Inteligencia etc, de igual manera que las operaciones de Comunicación Social, Operaciones en Apoyo a la Información e Inteligencia, según la finalidad buscada para su empleo.

Comparten similares Principios, coincidiendo en la conducción de las operaciones al más alto nivel de que se trate, con un planeamiento centralizado y ejecución descentralizada por Células, necesidad de estricta coordinación de los medios empleados, oportuna y detallada inteligencia, una planificación basada en efectos, y una preparación anticipada a las acciones. La comparación finaliza detallando una composición similar de las Células que ejecutarán las acciones.

Capítulo III: Propuesta de una organización

“El verdadero soldado no lucha por que odia lo que tiene delante, sino porque ama lo que tiene detrás.” (G.K. CHESTERTON, s.f).

En este último capítulo, se buscará precisar cuáles son los elementos necesarios que deben integrar una organización para operar en un ambiente de la Guerra de la Información a nivel operacional a los efectos de diseñar una estructura eficiente a tal fin, a la luz de las disponibilidades actuales del IMT y eventualmente determinar la necesidad de la creación de nuevos elementos.

El mismo se estructura en 3 secciones, donde en la primera se busca abordar los principales efectos a lograr con las Operaciones de Información. En la segunda sección se enumeran los elementos orgánicos del IMT y los propuestos a crear, para lograr los efectos deseados vistos en la primera sección. Subsiguientemente en la 3ra sección se propondrá una organización de estos elementos, y su funcionamiento, cerrando el capítulo con un apartado de conclusiones parciales.

Sección 1: Efectos que se pueden alcanzar con las Operaciones de Información

El reglamento de la Conducción para las Fuerzas Terrestres (ROB-00-01), como ya se advirtió, no contempla el desarrollo de este tipo de operaciones, por lo tanto, en esta Sección, se tomará como guía el PDC -39 Doctrina Conjunta de Targeting, del Ejército Español, en razón de que en su contenido existe una clasificación de los efectos a alcanzar con las Operaciones de Información explicada detalladamente, con la cual se está de acuerdo para que sea incluida en esta investigación.

Seguidamente se expondrán los aspectos que más interesan, a modo de resumen, del reglamento español citado:

Generalidad:

“Un efecto es el estado físico o de comportamiento de un sistema como resultado de una acción, conjunto de acciones u otro efecto sobre él. Los efectos letales se pueden alcanzar mediante diferentes acciones” (Estado Mayor de la Defensa, 2014), art.02039)

Los efectos pueden ser de dos categorías.

Deseado: Son los que se pretende lograr, y están en directa vinculación con los objetivos estratégicos y estado final deseado.

No Deseados: Estos pueden ser positivos o negativos, y afectan significativamente el logro del objetivo propuesto y el estado final deseado. Estos pueden producirse por acciones del enemigo o por consecuencias no intencionadas propias, acá entra en juego la intromisión de variable no relevante, que emergen como situaciones no contemplada en los planes, ocupando un papel relevante en el desarrollo de las operaciones. Si bien hay planes de contingencia que están contempladas en la matriz de sincronización y en las pautas de control, son hechos puntuales que no se tuvieron en cuenta y ante estímulos resurgen de manera significativa.

A su vez los efectos nombrados pueden producirse en forma directa o indirecta.

Efectos directos: Son fáciles de identificar, por lo general son de primer orden, inmediatos, producto de acciones militares y normalmente estos efectos son deseados.

Efectos indirectos: Son difíciles de reconocer o identificar, son efectos de segundo, tercer orden o mayor con efectos retardados que se producen por acciones, eventos o mecanismos intermedios.

Una vez mencionada en forma general de la clasificación de los efectos, nos vamos a referir sobre la afectación que se puede lograr.

Efectos basados en el daño:

Letales: Producen un daño físico irreversible del blanco, pierde su capacidad de recuperación, queda fuera de combate en forma permanente.

No letales: Son aquellos blancos que se alcanzan logrando un daño físico parcial recuperable.

Efectos basados en su naturaleza.

Físicos: Son todos los blancos en que se puede lograr su destrucción total, parcial o afectando sus capacidades funcionales.

Sistémicos: Busca afectar las funciones de uno o varios sistemas determinados. Requiere un mayor esfuerzo para la obtención de la información e inteligencia que los físicos, por la necesidad del conocimiento del sistema a afectar que podrán ser difícilmente observables. Si bien es más difícil poder detectar cual es el engranaje principal o aquella pieza que hace funcionar al sistema, afectándolo se logra un disloque en los lazos de funcionabilidad. La afectación estará supeditada al tiempo, la inteligencia que uno pueda realizar y la tecnología a disposición.

Comunicación Social: Son aquellos efectos que tienden a afectar sobre la toma de decisión del adversario como así también en su espíritu combativo. Busca la mente del adversario, por lo tanto, es más difícil de medir que los anteriores, ya que pueden tener un efecto indirecto. (El Art.02043 del reglamento en estudio, lo enuncia como Psicológicos)

Efectos basados en la interacción del blanco con su entorno o sistema.

Acumulativos: Varios efectos directos acumulados, obtendrán mayor resultado que la suma de los efectos inmediatos.

En cascada: Se producen en un sistema o conjunto de sistemas interrelacionados, a través de nodos críticos.

Colaterales: Son consecuencias no intencionales que producen daño a personas u objetos no relacionados con el objetivo donde se actúa.

Los efectos, como sea expuesto, no solo van a influir sobre objetivos físicos, sino que también sobre objetivos blandos, afectando y alterando la toma de decisiones del adversario, y

en muchos casos influyendo sobre su estado moral en forma negativa y potenciando la propia (Estado Mayor de la Defensa, 2014). Arts. 02024 al 02044)

Sección 2: Elementos idóneos para operar en la Guerra de la Información orgánicos del IMT y a crear.

Orgánicos del IMT.

Inteligencia. Cada nivel de comando, segregará de su elemento de Inteligencia dependiente, el personal y material necesario para integrar la Célula, a los efectos de, dirigir e integrar los medios de ejecución de inteligencia, procesar la información obtenida y producir inteligencia para el planeamiento y conducción de las operaciones, dirigir y coordinar y controlar las medidas de seguridad de contrainteligencia, y diseminar y usar la inteligencia resultante. (Ejército Argentino, Inteligencia Tactica, 2008)

Guerra Electrónica. Como determina nuestro reglamento de Conducción de Fuerzas Terrestres, otro elemento idóneo es el batallón de Guerra electrónica, cuya misión principal es controlar el espacio electromagnético, apoyando a las propias fuerzas y atacar la del enemigo en este ambiente.

Si bien este elemento responde al más alto nivel de la conducción, eventualmente podrá apoyar al nivel táctico para cumplir misiones específicas.

El sistema táctico de Guerra Electrónica debe estar en apoyo al Componente Terrestre del Teatro de Operaciones, a su vez será complementado por sistemas de armas de elementos de Artillería y de Aviación de Ejército. Como así también todas las tropas del Teatro de Operaciones deben estar en capacidad de realizar acciones de protección electrónica.

Tropas de Operaciones Especiales. Otra herramienta útil que cuenta el comandante para desarrollar este tipo de operaciones son las Tropas de Operaciones Especiales, las cuales están equipadas, adiestradas e instruidas para operar detrás de las líneas del enemigo afectando sensiblemente blancos de alto valor estratégico. Estas tropas están conformadas por Comandos,

Cazadores de Montaña y Cazadores de Monte que de acuerdo al ambiente geográfico o la misión a cumplir serán asignadas o agregadas al Teatro de Operaciones. (Ejército Argentino, Conducción para las Fuerzas Terrestres (ROB - 00 - 01), 2015)

Fuerzas Especiales. Por otro lado, debemos mencionar a la Fuerzas Especiales, que si bien pueden realizar operaciones directas como los elementos que mencionamos anteriormente, estas tropas están en capacidad de potenciar e influir en forma más adecuada en el ambiente que nos ocupa. Principalmente dentro de sus operaciones podemos mencionar a las COSACO que busca como actividad principal, lograr un cambio de conducta sobre las posibles percepciones que pueda desarrollar la fuerza propia, las enemigas y la población local, como así también, incrementar la voluntad de lucha y afectar la capacidad de combate del oponente. (Ejército Argentino, Manual de Técnicas y Procedimientos para Fuerzas Especiales, 2015)

Ciberdefensa. Otro elemento recientemente incorporado a la estructura del Estado Mayor Conjunto de las Fuerzas Armadas, es la Ciberdefensa que tiene como finalidad principal la de prevenir, detectar, identificar, anular, evitar, contrarrestar, contener o repeler una amenaza cibernética. (Ejército Argentino, Conducción para las Fuerzas Terrestres (ROB - 00 - 01), 2015)

Las actividades de Ciberdefensa constituirán una herramienta fundamental en la configuración de probables amenazas, definiendo este sistema como una mutación exponencial que busca anticiparse a las recientes tecnologías empleadas como amenazas, que son elaboradas con sistemas que buscan solaparse en monitoreo que se realiza en el campo de combate.

Elementos a crear o requerir.

Centro de asesores comunicacionales y prensa. Compuesto por psicólogos, antropólogos, sociólogos y periodistas, incorporados a la fuerza o requerimiento de un organismo relacionado a la Fuerza.

Como misión general podemos mencionar que tendrá la función de asesorar e intervenir en las Operaciones de Información respecto a las condiciones de salud mental del personal de

la fuerza y eventualmente como afectar la del oponente a través de diferentes mecanismos de comunicación, utilizando el mensaje, propaganda, publicidad, radiofonías, radio estaciones, medio masivos de redes (Twitter, Instagram, Facebook) entre otros.

Como así también evaluar la ausencia de síntomas psicopatológicos del personal que se encuentra desplegado en la zona de combate para mantener la aptitud y actitud.

Estructurar un mensaje requiere una alta complejidad que debe estar supervisada necesariamente por profesionales que sean idóneos en el tema, Más allá de preguntarse ¿Para quién va dirigido? ¿Cuál será el impacto mediático? ¿Qué efectos puedo provocar? ¿A qué público está dirigido? ¿Qué se quiere afectar? ¿Cuánto tiempo debe durar el efecto?, que son interrogante validos a la hora de formular la acción, es de suma importancia que el mensaje a enviar, no afecte a la propia tropa, ya que se obtendría un efecto contrario al deseado.

Otro aspecto a mencionar es la incorporación de prensa, con la siguiente salvedad, de que hay diferentes niveles, periodista acreditado, corresponsal militar y corresponsal de guerra siendo este último el más apto para integrar la célula en operaciones.

Inicialmente se seleccionará periodistas civiles donde se lo acreditará mediante exigencias sobre notas, entrevistas y cobertura de interés de la fuerza, una vez cumplida esta etapa se le propondrá a que realice el curso de corresponsal militar realizando ejercicios y trabajando como un periodista que acompaña a la fuerza durante las diferentes ejercitaciones. Cuando se establece el Teatro de Operaciones legalmente ese corresponsal militar se lo movilizará como corresponsal de guerra.

Los periodistas formadores de opinión serán de gran utilidad a la hora de concientizar al público interno sobre las operaciones en desarrollo o a desarrollar para lograr su adhesión.

Sección 3: Organización de un elemento para la Guerra de la Información.

La organización más conveniente para este tipo de elemento multidisciplinario, es el fractal ya que es indispensable que sus componentes cuya característica es la heterogeneidad

en cuanto a la naturaleza de sus funciones, operen en forma fluida, flexible, interrelacionada, sincronizada e integrada. Para ello lo más adecuado es concebir una estructura del tipo celular para un eficiente funcionamiento

Estas Células, deben responder a los criterios para organización de las fuerzas (Interoperabilidad / Modularidad / Flexibilidad / Sustentabilidad), ya que constituyen elementos de combate/técnicos equipados y adiestrados, para ejecutar operaciones de naturaleza compleja, normalmente asociadas a objetivos estratégicos vitales o tácticos, coincidentes con los efectos perseguidos normalmente por las Operaciones de Información, que están dirigidas a obstaculizar el sostenimiento de las operaciones enemigas, sus vías de comunicación y a su comando y control, todo esto con la finalidad de limitar la libertad de acción, alterar el ritmo y la coherencia de las operaciones y aislar sus fuerzas.

Propuesta de organización de una Célula y su funcionamiento.



Figura 1. Propuesta de una Organización para operar en un ambiente de la Guerra de la Información.

Como podemos observar en la figura 1, la estructura de esta Célula es en forma circular donde la información es compartida por todos los integrantes de la misma. Quien regula el flujo será el oficial de Operaciones de Información (G3I). Otro aspecto importante a mencionar es que al tener una estructura fractal se puede regenerar tantas veces como sea afectada como así también adaptar su estructura de acuerdo a los efectos deseados a lograr. Es por ello que ésta es la mejor manera de generar diferentes capacidades de autonomía y autosuficiencia.

Dentro de su funcionamiento, primero debemos delimitar el alcance de las responsabilidades del Jefe de Célula. Dependerá del Oficial de Operaciones y estará en estrecha relación con el área de Inteligencia. Tendrá como responsabilidad principal asesorar al área de Operaciones en todo lo concerniente a las Operaciones de Información, a través de los elementos puesto a disposición con la finalidad de proteger las propias operaciones y afectar las capacidades de comando, control, comunicaciones e inteligencia del enemigo. Como así también, aquellos medios físicos que pongan en peligro la propia misión.

Como principal aspecto a mencionar dentro de su funcionamiento, debemos decir que los requerimientos que lleguen a la Célula de Operaciones serán a través de efectos, donde se iniciara un proceso mediante el cual se seleccionarán los posibles blancos, se los valorizarán dando prioridades, se verá que acciones se pueden realizar sobre ellos y posteriormente se ejecutarán la acciones pertinentes para cumplir con lo solicitado, y posteriormente se hará una valorización del resultado sobre el efecto solicitado.

Ya adentrándonos de lleno a la mecánica de la Célula, tenemos que mencionar que, al conformarse el Teatro de Operaciones, éste va estar integrado por distintas organizaciones con un orden de batalla para operar en ese ambiente particular, sin una organización fija, estructurado acorde a las funciones geoestratégica de interés y de acuerdo a la misión impuestas, es así, que estas organizaciones deberán responder a los principios de configuración y congruencia.

Una vez conformado el Comando Terrestre del Teatro de Operaciones, integrará en su Orden de Batalla la Célula de Operaciones de Información compuesta por elementos de Inteligencia, fracciones de Asuntos Civiles, Fuerzas Especiales, Tropas de Operaciones Especiales, Elementos de Guerra Electrónica, elementos de Ciber guerra, elementos de Comunicaciones y toda aquella organización militar o civil especializada, armamento y equipos especiales, necesarios para lograr el efecto deseado, acorde a la misión impuesta.

Conclusiones parciales

Dentro del diseño de toda operación se determinan las diferentes líneas de operaciones que van a concatenar las diferentes acciones hasta afectar el centro de gravedad del enemigo.

Nuestra doctrina no se ocupa de las Operaciones de Información, por lo tanto, no existen líneas de operaciones de esta temática en especial creando una debilidad a la hora de operar, ya que, de este tipo de operaciones, sí, se ocupan los principales ejércitos regionales y las principales potencias de orden mundial

El elemento a crear deberá desarrollar un numeroso conjunto de actividades antes del despliegue de la Fuerza, creando las condiciones necesarias para reducir el impacto de las acciones por parte del enemigo. Es por ello que es gravitante que al momento de movilizarse esta estructura deberá estar adecuadamente equipada y adiestrada desde la paz.

Este elemento, sin darle una denominación concreta, será del tipo celular, ya que por sus características de empleo esta organización facilita que se opere en forma fluida, flexible, interrelacionada, sincronizada e integrada.

El IMT dispone en su orgánica de elementos idóneos para formar las Células, pero no están interrelacionados ni operan bajo un comando único para la planificación de los efectos a lograr y la conducción de las Operaciones de Información. Para integrar una célula eficiente, a los elementos orgánicos debidamente adiestrados e interrelacionados bajo un comando único,

es necesario completarla con especialistas del ámbito militar y también del civil, especialmente en lo que se refiere a prensa, acción cívica, psicólogos, sociólogos, etc.

Queda expuesto que el factor crítico de esta nueva organización va a ser el personal de especialistas necesarios para ejecutar las diferentes acciones que conforman la Guerra de la Información. Es por ello que se hace hincapié en la formación de estos técnicos profesionales, utilizando como pilar fundamental la Facultad de Ingeniería de le Ejército, la Secretaria General del Ejército, la Escuela de Tropas Especiales y Aerotransportadas, Aviación de Ejército, el arma de Comunicaciones y Asuntos Civiles entre otros.

Conclusiones finales

A lo largo de esta investigación, se abordaron los temas que hacen al objetivo general fijado para este trabajo cual es “Determinar la estructura de una organización del IMT a nivel operacional, para desarrollar las distintas funciones que debe ejecutar en un ambiente de la Guerra de la Información.”, en un todo de acuerdo al tema impuesto “Desarrollo de capacidades del Instrumento Militar Terrestre para operar en un ambiente de la Guerra de la Información”.

Para ello se incluyeron las distintas definiciones de Guerra de la Información, que tipo de operaciones se ejecutan, en que momento del desarrollo del conflicto tendrá mayor preponderancia, cual es la reglamentación extranjera que orienta a sus respectivos ejércitos. Se ejemplificó su uso en distintos escenarios bélicos en la historia de guerra reciente, se revisaron las leyes nacionales directamente implicadas para determinar si existen impedimentos para su empleo, se analizó en función a las operaciones a realizar, que elementos del IMT propio está en capacidad de concretarlas, cual es la organización más apta a crear y con cuales elementos humanos y técnicos con que se la debe completar para su eficiente funcionamiento, proponiendo gráficamente una probable organización.

A modo de conclusión, se puede afirmar que el dominio y preponderancia de acciones eficaces del Operaciones de Información para lograr el o los efectos deseados por el comandante, en un ambiente de la Guerra de la Información, será una herramienta valiosa, indispensable, vital para lograr disminuir el poder de combate del oponente y como factor multiplicados del propio.

No tener en cuenta lo expresado en el párrafo anterior, expondría a nuestras fuerzas a la acción del adversario, que sí contempla en su doctrina este tipo de acciones, colocándonos en una situación de desventaja abrumadora, ya que actuaría coordinadamente sobre nuestro C3I2 dominando el espectro electromagnético, lugar donde se desarrollan un sin número de tareas para controlarlo, considerándolas sin temor a equivocación como verdaderos combates

electrónicos. Este dominio le permitiría, además, actuar sin una oposición eficaz sobre el público interno y externo, para disminuir su moral, sin la debida protección de información de nuestras propias operaciones.

Es dable esperar, que, en un escenario de guerra actual, se actuará necesariamente en un ambiente de Guerra de la Información como una parte indispensable constitutiva del todo, ya que ésta, en forma incruenta y solapada, se puede utilizar para lograr los efectos deseados, antes, durante y después del conflicto con eficaces resultados, multiplicando el poder de combate del que la use y prevalezca sobre el oponente sin mayores esfuerzos ni costos pecuniarios, humanos y materiales ya que lo que se usa es el espacio cibernético, ilimitado en su dimensión, solo limitado por la tecnología disponible, el correcto uso de ella, y la actitud del comandante, coadyuvando así valiosamente a las operaciones militares en desarrollo o a desarrollar.

Estas operaciones se deben contemplar en todos los niveles de la conducción, tanto en el nivel Estratégico Militar, Estratégico Operacional y Táctico, utilizando los medios puestos a disposición, en cada uno de los niveles, con adecuada sincronización y requiriendo de todo conductor, un espíritu creativo, previsor, inteligente y audaz, ya que el mal empleo de las acciones, ya sea equivocándose en el efecto deseado, en el empleo técnico de los medios y/o su uso fuera de oportunidad, ocasionará un efecto contrario al deseado.

¿Cuáles son los efectos deseados en general? Sin detenernos en el cómo, que no es el motivo de esta investigación, el comandante buscará dominar el espectro de información del oponente oportunamente y proteger las propias creando así las condiciones para estar siempre “un paso adelante” de las acciones enemigas, dificultarlas, descoordinarlas y en lo posible impedirselas, para lograr así la iniciativa imponiendo el propio ritmo a las operaciones.

Es importante señalar que las Operaciones de Información, si bien pueden ser ofensivas y defensivas, su actividad no depende del tipo de operación en desarrollo en el campo de batalla,

ya que, en una operación ofensiva, se podrá utilizar técnicas defensivas de las Operaciones de la Información y viceversa, pero sí tendrán una visible influencia sobre todas ellas

El nivel de conducción más idóneo para coordinar y valorar los resultados de las Operaciones de la Información es el nivel Estratégico Operacional, ya que en el nivel Estratégico Nacional/Militar se elabora la estrategia a seguir dando una orientación general de cómo lograr los efectos estratégicos deseados.

En el nivel Operacional se efectuará la concepción, planificación y dirección de las operaciones y evaluación de los resultados, fijando a los diferentes componentes de la Célula los objetivos donde actuar y los efectos a lograr. Orienta y dirige a su vez al nivel Táctico. Por todas estas características se concluye que este nivel es el más apto y mejor ubicado dentro de la conducción para la concepción, planeamiento, impartición de las directivas y ordenes, efectuar el control y la evaluación de las Operaciones de Información que se desarrollen en apoyo a la maniobra dentro del campo de batalla.

El marco legislativo interno, en general no afecta al eventual empleo de las Operaciones de Información, pero sí, es necesario cubrir un vacío legislativo en cuanto al eventual empleo de las Operaciones de Información antes del conflicto a modo de disuasión y Alerta Temprana Estratégica” (DPDN, 2021), y especialmente para proteger el sistema propio de C3I2. De la misma manera, la ley 24.059 de Seguridad Interior, art. 32° inc. c), pone un límite al eventual empleo de las FFAA, en caso de extrema gravedad en el marco interno, al no permitir una adaptación en la doctrina, organización, equipamiento y capacitación, para enfrentar esa eventualidad.

Los principales ejércitos regionales y de las principales potencias mundiales contemplan la Guerra de la Información en su doctrina. En nuestro caso, casi nada hay escrito al respecto, solo breves menciones en el ROB-00-01 Conducción de las Fuerza Terrestres, lo que nos coloca en clara desventaja en caso de tener que operar ante agresiones externas

En el Capítulo 3, se propone la creación de una organización del tipo celular (ver gráfico 1), como la más apta para este tipo de operaciones, ya que se requiere que opere en forma fluida, flexible, interrelacionada, sincronizada e integrada. Su composición es heterogénea y multidisciplinaria, conformándose con elementos orgánicos del IMT y otros a crear o requerir.

Su dependencia será del área de Operaciones con una marcada integración con el área de Inteligencia. El nivel de comando más apto para el planeamiento, dirección y control de las operaciones y su evaluación es el Estratégico Operacional.

Los requerimientos para su empleo deberán llegar a través de los efectos que se desean lograr.

Es imprescindible la materialización de la creación de esta organización, a los efectos de una adecuada integración de sus componentes y su capacitación. Es dable esperar que el factor crítico sea el conseguir y adiestrar a los especialistas, que demandará tiempo y esfuerzo, pero si bien es dificultoso, es necesario.

Nuestras Fuerzas Armadas, vivieron durante la Guerra de Malvinas, una clara desventaja operacional especialmente de medios de todo tipo con Gran Bretaña. Uno de los factores que impactó silenciosa pero efectivamente, fue el dominio de espectro electromagnético, logrando con ello ubicación de tropas, armas propias en tiempo real, detección de radares, interferencia de las comunicaciones, escuchas, y todo tipo de operaciones que la tecnología del momento les permitía. Esa desventaja fue suplida por el factor humano, mediante valor e ingenio.

El hombre siempre será irremplazable porque es el que en definitiva decide, empleando razonamiento, criterio y rasgos de personalidad que no lo puede sustituir la técnica. Pero, y aunque parezca contradictorio, desde 1982 a la fecha la tecnología ha crecido exponencialmente, transformando el ciberespacio en un campo de batalla a conquistar y dominar si se quiere vencer, disminuyendo pero no anulando ese factor humano que en la

Guerra por la Independencia y en Malvinas hizo la diferencia, no se puede demostrar el coraje y valor, característica esencial del soldado argentino en toda su historia, contra un silencioso misil lanzado desde una aeronave no tripulada guiada a miles de kilómetros del blanco, que va a destruir con alta precisión su objetivo sin que sus ocupantes lo hayan advertido.

“Un viaje de mil millas, comienza con solo un paso.” (Lao Tse Filósofo chino, S IV a. C.)

Aporte Profesional

Se entiende como capacidad a la aptitud o factores suficientes que poseyera una organización o individuo para realizar una determinada acción, función, misión u otra cosa. Hemos visto a lo largo de la investigación, que el Instrumento Militar Terrestre carece de capacidades para poder desarrollar con total plenitud este tipo de operaciones, no solo por las limitaciones legales y tecnológicas, sino también por la ausencia de organización, educación, instrucción y adiestramiento. Es por ello, como dice el Reglamento Conducción para las Fuerzas Terrestres, que la preparación para la guerra será el hilo conductor para todas las actividades que realice una organización militar y sus elementos dependientes, para lo cual es de vital importancia que esta organización celular este prevista desde la paz para afrontar el acontecimiento social más espectacular y violento, la guerra, “procurando afectar las menores adecuaciones posibles al ser desplegado para la ejecución de operaciones.”(Ejército Argentino, Conducción para las Fuerzas Terrestres (ROB - 00 - 01), 2015, pág. 38)

La tecnología de avanzada, será el factor común en la composición de las Células, pero, el hombre seguirá siendo el eje central como en cualquier otra operación, por lo tanto, su preparación debe ser permanente para desempeñarse con eficiencia en este ambiente particular; para ello, es necesario realizar en los diferentes niveles de comando, ejercitaciones con los distintos equipos que conformarán este tipo de organización al menos 2 veces al año.

Si bien el nivel más apto para conducir la Operación de información es el operacional, no debemos olvidar que éste también se desarrolla en el nivel táctico, por lo tanto se infiere, que es menester incluir en los programas de educación, de los centro de formación de oficiales y suboficiales la temática en cuestión, como así también realizar las ejercitaciones en los diferentes institutos de perfeccionamiento, ya sea incluyendo dentro de la distribución de los roles de combate los puestos correspondientes a los integrantes de la Célula, en el marco del ejercicio a desarrollar, o implementando ejercicios exclusivos dentro de un ambiente de la Guerra de la Información.

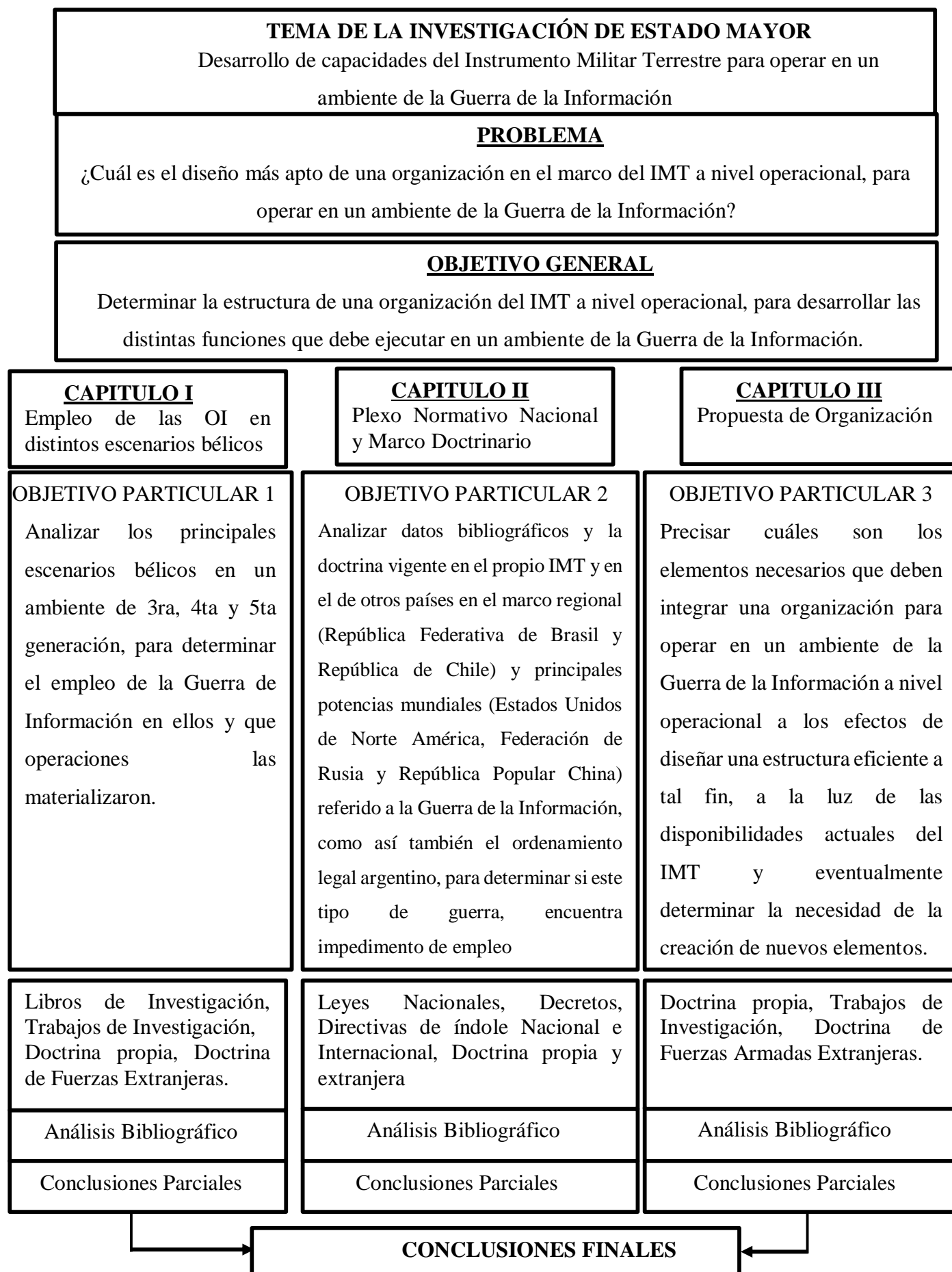
Referencias

- Ángeles, Ernesto. (05 de Octubre de 2021). *El ciberespacio chino en la ciberguerra. La guerra de la información.* Obtenido de https://www.academia.edu/26032548/El_ciberespacio_chino_en_la_ciberguerra_La_guerra_de_la_informaci%C3%B3n?auto=download
- BBC, N. (5 de Octubre de 2021). *Muerte de Qasem Soleimani: cómo fue el "ataque de precisión" en el que EE.UU. eliminó el militar más poderoso de Irán (y qué hay detrás).* Obtenido de <https://www.bbc.com/mundo/noticias-internacional-50989553>
- BBC, NEWS. (05 de Octubre de 2021). *Por qué Israel reconoce por primera vez que destruyó un reactor nuclear en Siria hace 11 años.* Obtenido de <https://www.bbc.com/mundo/noticias-internacional-43486931>
- Campos, G. (2021). Curso de Oficial de Estado Mayor. *Materia: Inteligencia Estratégica.* Buenos Aires, Argentina: Escuela Superior de Guerra del Ejército Argentino.
- Capanegra, Julian. (05 de Octubre de 2021). Operacion Overlord. *Operaciones de configuración.* Buenos Aires, Argentina: Escuela Superior de Guerra.
- Clarín. (05 de Octubre de 2021). *SEGURIDAD INFORMATICA: VULNERO LOS SISTEMAS INFORMATICOS DE LA MARINA DE ESTADOS UNIDOS.* Obtenido de Habla el hacker argentino que puso en jaque al FBI: https://www.clarin.com/sociedad/habla-hacker-argentino-puso-jaque-fbi_0_SkaeFh6gRKx.html
- Crimen de agresión. (05 de Octubre de 2021). *Resolución 3314 de las Naciones Unidas sobre definición de la agresión.* Obtenido de <http://www.derechos.org/nizkor/aggression/doc/aggression38.html>
- Derleth, D. (05 de Octubre de 2021). *La guerra de nueva generación de Rusia, Disuadir y ganar en el nivel táctico.* Obtenido de <https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/2Q-2021/Derleth-SPA-Q2-2021-A.pdf>
- Do Amarante, J. (2014). *El vuelo de la Humanidad.* Buenos Aires: + Letras Comunicaciones.
- Ejército Argentino. (2008). *Inteligencia Tactica.* Buenos Aires: Departamento Doctrina.
- Ejército Argentino. (2015). *Conducción para las Fuerzas Terrestres (ROB - 00 - 01).* Buenos Aires: Departamento Doctrina.
- Ejército Argentino. (2015). *Manual de Técnicas y Procedimientos para Fuerzas Especiales.* Buenos Aires: Departamento Doctrina.

- Ejército Argentino. (2020). Especialización en Historia Militar Contemporánea. *Materia: 4*. Buenos Aires, Argentina: Escuela Superior de Guerra.
- Ejército de Chile. (2010). *Operaciones de Información (EB20 - MC - 10.215)*. Santiago de Chile: División Doctrina.
- Estado Mayor de la Defensa. (2014). *DOCTRINA CONJUNTA (PDC – 3.9)*. Madrid: Estado Mayor de la Defensa.
- Ferrari, Vigón, Gaggero. (2001). Curso de Formación de Oficial de Estado Mayor. *La Revolución de Asuntos Militares y la Guerra de la Información*. Buenos Aires, Argentina: Escuela Superior de Guerra.
- Infobae. (05 de Octubre de 2021). *La increíble historia del "hombre que nunca existió" que cambió el curso de la Segunda Guerra Mundial*. Obtenido de <https://www.infobae.com/america/historia-america/2018/05/02/la-increible-historia-del-hombre-que-nunca-existio-que-cambio-el-curso-de-la-segunda-guerra-mundial/>
- InfoLeg. (5 de Octubre de 2021). *Agencia Federal de Inteligencia*. Obtenido de <http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm>
- InfoLeg. (5 de Octubre de 2021). *Defensa Nacional*. Obtenido de Ley N° 23.554: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm>
- InfoLeg. (5 de Octubre de 2021). *Ley de Inteligencia Nacional*. Obtenido de Ley 25.520: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm>
- InfoLeg. (5 de Octubre de 2021). *Seguridad Interior*. Obtenido de Ley N° 24.059: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/458/texact.htm>
- Owen, Mark. (2012). *Un Día Difícil*. Buenos Aires: Crítica.
- Schnessel, S. (05 de Octubre de 2021). *Enlace judío*. Obtenido de Todo sobre el ataque al reactor nuclear de Siria que Israel destruyó: <https://www.enlacejudio.com/2018/04/14/ataque-reactor-nuclear-siria-israel/>
- Spretz, Norberto Ivan. (2018). ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO. *Las operaciones de información de nivel operacional y su influencia en el ambiente informacional*. Buenos Aires: Escuela Superior de Guerra Conjunta.
- Stella, Facundo. (2015). Curso de Oficial de Estado Mayor. *Las Fuerzas de Operaciones Especiales del Ejército Argentino y su vinculación orgánica*. Buenos Aires, Argentina: Escuela Superior de Guerra de Ejército Argentino.
- Sun Tzu. (2014). *Arte de la Guerra*. Buenos Aires: Centro Editor de Cultura.

- Tepedino, Sebastián. (05 de Octubre de 2021). *Espacio Estratégico*. Obtenido de La Doctrina Guerásimov, ¿Un salto cuántico en la teoría militar rusa?: <http://espacioestrategico.blogspot.com/2019/03/la-doctrina-geramismov.html>
- Tovar, H. L. (5 de Octubre de 2021). *GUERRA DE INFORMACIÓN*. Obtenido de ¿El arma es el mensaje? (Tesis completa): https://www.academia.edu/34113445/GUERRA_DE_INFORMACI%C3%93N_El_arma_es_el_mensaje_Tesis_completa_
- USA Joint Chiefs of Staff. (1988). *Joint Doctrine for Information Operations (USA JOINT PUP 3-13)*. US Military.
- USA Joint Chiefs of Staff. (2011). *Joint Operation Planning (JP 5-0)*. US Military.
- USA Joint Chiefs of Staff. (2012). *Information Operations (JP 3-13)*. US Military.
- USA Joint Chiefs of Staff. (2017). *Joint Operations (JP 30-0 17)*. USA: US Military.
- Wikipedia. (5 de Octubre de 2021). *Guerra de Yom Kipur*. Obtenido de https://en.wikipedia.org/wiki/Guerra_de_Yom_Kipur
- Wikipedia. (5 de Octubre de 2021). *Information warfare*. Obtenido de https://en.wikipedia.org/wiki/Information_warfare
- Wilhelm, Tom. (5 de Octubre de 2021). *Revista Profesional del Ejército de EUA*. Obtenido de Planteamiento de las Fuerzas Armadas rusas sobre el empleo de la influencia en períodos de competencia: <https://www.armyupress.army.mil/Journals/Edicion-Hispanoamericana/Archivos/Segundo-Trimestre-2021/Wilhelm-Planteamiento/>

Anexo 1 (Esquema Gráfico Esquemático)



Anexo 2: (Entrevista Nro 1). a la Investigación de Estado Mayor TC Álvaro ACHONDO de la ESG (Profesor).

ENTREVISTA PARA EL TRABAJO FINAL INTEGRADOR DEL Mayor Mariano Agustín LOSITO DE LA ESG.

APELLIDO y NOMBRE	ACHONDO Álvaro
Grado	Teniente Coronel
Rol que ocupa actualmente	Profesor invitado

1. Tema del trabajo final integrador:

“Desarrollo de capacidades del Instrumento Militar Terrestre para operar en un ambiente de la Guerra de la Información” (TC Achondo)

- a. ¿En base a su conocimiento profesional sobre la dinámica del campo de combate moderno, cual es la importancia que usted la asigna a la Guerra de la Información dentro de este?

La planificación de operaciones de información, se caracteriza por constituir un proceso de análisis, integración e interpretación de información detallada de cada una de las capacidades de Operaciones de Información. Es fundamental tener en cuenta la prioridad de los objetivos que se persigan en cuanto a requerimientos prioritarios de inteligencia. Obedece a un proceso continuo cíclico.

- b. ¿Puede usted mencionar alguna operación dentro del marco de la Guerra de la Información, que haya sido utilizada por su país dentro del territorio nacional o en el extranjero, en caso de haberla realizado mencione que tipo de operación se realizó, que efectos obtuvo?

Operaciones de Información relacionadas con:

- Cooperación cívico militar (CIMIC).
- Información pública (PI).

Lo anterior, enmarcado en actividades que la fuerza debió desarrollar en el marco de las emergencias, catástrofes y desastres naturales acaecidos en Chile.

- c. ¿A su criterio, cual sería a grandes rasgos la organización más eficiente para operar en un ambiente de Guerra de información?

Los rasgos serán aquellos que le permitan a la unidad ejecutar operaciones de información, las que serán esenciales para la ejecución exitosa de las actividades militares. Su objetivo fundamental será coadyuvar al esfuerzo de la maniobra de la fuerza, con la finalidad de dominar, mantener, controlar y alcanzar la superioridad de las informaciones.

- d. A su entender ¿cuál son la ventajas y desventajas de ejecutar estas actividades antes, durante y después del conflicto? ¿Por qué?

Las ventajas podrán ser permanentes al ejecutar Operaciones de Información en forma continua y dinámica cuyo propósito de dominar, mantener, controlar y alcanzar la superioridad de las informaciones.

- e. ¿Desea agregar algo que considere de importancia mencionar?

Anexo 3: (Entrevista Nro 2) a la Investigación de Estado Mayor Renato TC BIONE DA SILVA de la ESG (Alumno).

ENTREVISTA PARA EL TRABAJO FINAL INTEGRADOR DEL Mayor Mariano Agustín LOSITO DE LA ESG.

APELLIDO y NOMBRE	MACEDO BIONE DA SILVA, Renato
Grado	Teniente Coronel (BRASIL)
Rol que ocupa actualmente	Cursante del COEM

1. Tema del trabajo final integrador:

“Desarrollo de capacidades del Instrumento Militar Terrestre para operar en un ambiente de la Guerra de la Información” (TC Bione Da Silva)

- a. ¿En base a su conocimiento profesional sobre la dinámica del campo de combate moderno, cual es la importancia que usted la asigna a la Guerra de la Información dentro de este?

Considero fundamental pues en el entorno operativo contemporáneo complejo y multifacético con numerosos actores, obtener y producir información y su la integración son esenciales para la supervivencia de las instituciones militares. Así que, el empleo de Fuerzas Terrestres no puede prescindir del establecimiento de conexiones que permitan obtener y / o producir los conocimientos necesarios para la efectiva toma de decisiones y realizar operaciones militares terrestres a fin de prevenir el surgimiento de amenazas. Por tanto, a los militares les interesa saber cómo tratar las fuentes que proporcionan datos y / o producen información para la gestión de crisis o la resolución de conflictos armados.

- b. ¿Puede usted mencionar alguna operación dentro del marco de la Guerra de la Información, que haya sido utilizada por su país dentro del territorio nacional o en el extranjero, en caso de haberla realizado mencione que tipo de operación se realizó, que efectos obtuvo?

Dentro del marco de las acciones ejecutadas por el Ejército Brasileño a fin de reducir los niveles de criminalidad existentes en la provincia de Rio de Janeiro, las Operaciones de Información fueron fundamentales para informar a población local los objetivos de la acción como un todo y explicar las reglas de enfrentamiento que fueron establecidas. Además, permitieron informar a la sociedad como los recursos financieros estaban siendo usados y

cuales resultados habían sido logrados por las fuerzas, permitiendo que la credibilidad y confianza en las Fuerzas Terrestres fuesen mantenidas en niveles elevados. Los resultados fueron en línea con los esperados y planificados inicialmente, haya vista que hubo una significativa colaboración por parte de la población local para que los objetivos propuestos fuesen alcanzados, bien como la sociedad comprendió la complejidad y dificultad que involucraban las operaciones que fueron realizadas.

- c. ¿A su criterio, cual sería a grandes rasgos la organización más eficiente para operar en un ambiente de Guerra de información?

-Estructura organizacional de planificación centralizada en el más alto nivel
 -Organización debe contar con equipos especializados en observar los efectos a lograr y su permanente evaluación sobre los objetivos, a corto, medio y largo plazo.
 -Integración de la organización con sistemas de inteligencia visando definir más claramente cuáles serían los efectos deseados en una determinada operación

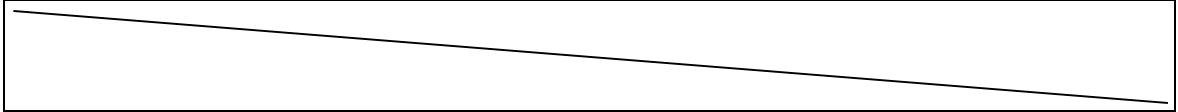
- d. A su entender ¿cuál son la ventajas y desventajas de ejecutar estas actividades antes, durante y después del conflicto? ¿Por qué?

Creo que las ventajas están relacionadas con la posibilidad de evitar acciones hostiles contra la fuerza, especialmente por parte de la población local durante las operaciones. Además, permite maximizar el poder de combate de la fuerza, al emplear eficazmente las capacidades requeridas de información, estas entendidas como las que permiten afectar la capacidad de los oponentes o potenciales adversarios para orientar, obtener, producir y / o difundir información.

Por otro lado, las desventajas están relacionadas con la posibilidad de que sean repasadas informaciones equivocadas, que, una vez transmitidas, tendrán reflejo negativo para las fuerzas durante toda operación y se tornará extremadamente costoso su reversión. Se suma también la posibilidad de que, al término de la operación, las Operaciones de Información

desencadenadas tengan un reflejo negativo entre la población influenciada y las fuerzas que actuaron.

e. ¿Desea agregar algo que considere de importancia mencionar?



Anexo 4: (Entrevista Nro 3). a la Investigación de Estado Mayor MY Héctor PADILLA de la ESG (Alumno).

ENTREVISTA PARA EL TRABAJO FINAL INTEGRADOR DEL Mayor Mariano Agustín LOSITO DE LA ESG.

APELLIDO y NOMBRE	PADILLA GONZÁLEZ, Héctor A.
Grado	MAY
Rol que ocupa actualmente	Alumno

1. Tema del trabajo final integrador:

“Desarrollo de capacidades del Instrumento Militar Terrestre para operar en un ambiente de la Guerra de la Información” (MY Padilla)

- a. ¿En base a su conocimiento profesional sobre la dinámica del campo de combate moderno, cual es la importancia que usted la asigna a la Guerra de la Información dentro de este?

La guerra de información es muy importante durante la planificación de las misiones dentro del Arma de Policía Militar debido a la información diseminada puede ser crítica para las misiones asignadas.

- b. ¿Puede usted mencionar alguna operación dentro del marco de la Guerra de la Información, que haya sido utilizada por su país dentro del territorio nacional o en el extranjero, en caso de haberla realizado mencione que tipo de operación se realizó, que efectos obtuvo?

Como jefe de operaciones durante la Campaña Fe en La Causa año 2012. Usamos la guerra de información en el Cauca y Larandia para evitar el reclutamiento de civiles para las guerrillas dentro del país. Esto beneficio en gran manera en como la población comenzó a ver a la guerrilla.

- c. ¿A su criterio, cual sería a grandes rasgos la organización más eficiente para operar en un ambiente de Guerra de información?

En el caso del Ejército de Estados Unidos, la unidad responsable por crear este tipo de operaciones es la Arma de Operaciones Psicológicas. Uno de los rasgos más importantes es conocer el leguaje y la cultura para adaptar planes a largo plazo.

- d. A su entender ¿cuál son la ventajas y desventajas de ejecutar estas actividades antes, durante y después del conflicto? ¿Por qué?

Estas operaciones deben ser continuas, en Afganistán se fracasó porque no se tenía

una actividad concreta en el comienzo. El plan se estableció durante el conflicto. Colombia es el vivo ejemplo de cómo se deben establecer este tipo de actividades para mantener un plan a largo plazo.

e. ¿Desea agregar algo que considere de importancia mencionar?

Las actividades de guerra de información deben ser adaptadas a la cultura y en el lenguaje popular. Información que sea muy complicada de entender y puede ser interpretada de diferentes maneras.

Anexo 5: Influencias de las operaciones durante el conflicto.

Teniendo una aproximación de definiciones y sus posibles operaciones, es oportuno establecer en qué momento se van a desarrollar estas operaciones y su preponderancia con mayor intensidad durante la concreción del efecto final deseado que va a constituirse como sinergia para obtener la victoria en la campaña/guerra.

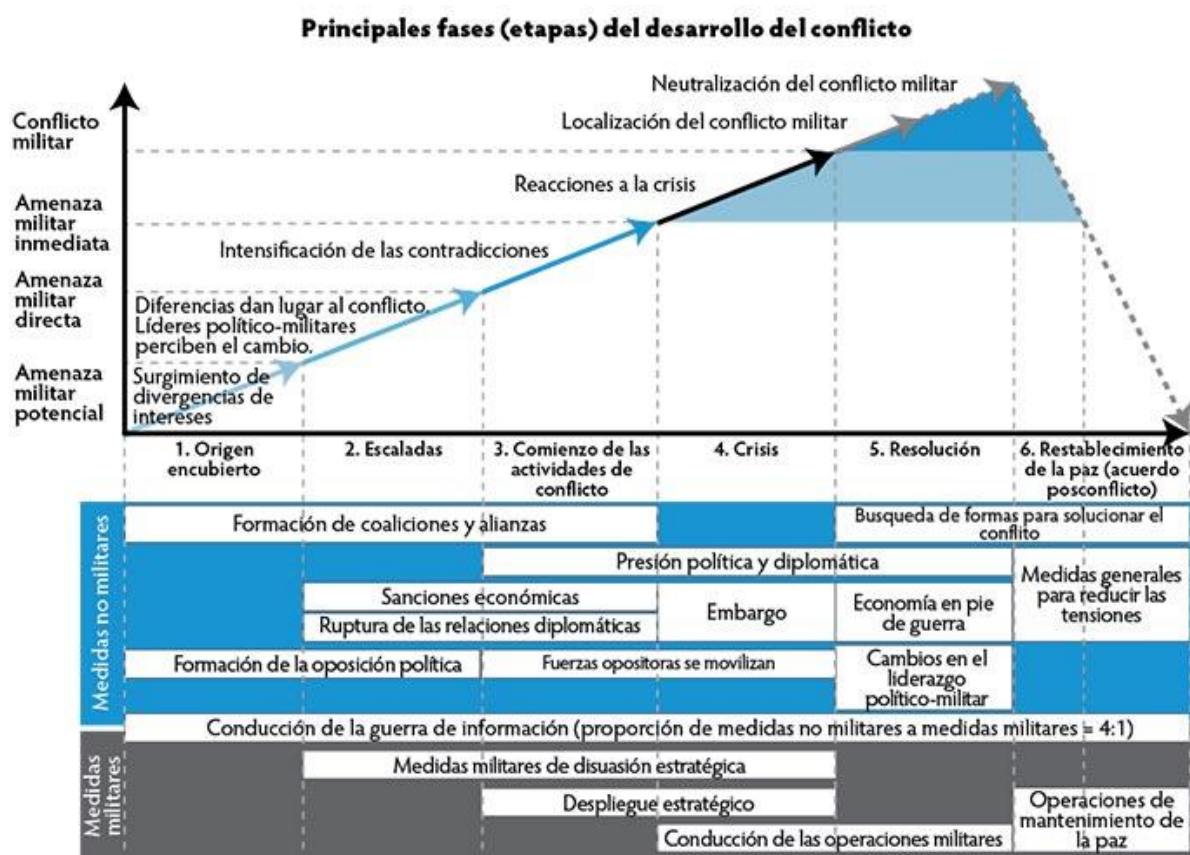


Figura 2. Grado de participación de las Operaciones de Información durante las distintas fases de la operación, marcando su rendimiento en la escala vertical y las distintas fases en la escala horizontal.

Fuente: <https://www.armyupress.army.mil/Journals/Edicion-ispanoamericana/Archivo-de-articulos-exclusivos-en-linea/Hispanoamericana-On-line-2018/acciones-Rusia/>