COMANDO CONJUNTO DE LAS FUERZAS ARMADAS
DIRECCIÓN DE EDUCACIÓN Y DOCTRINA MILITAR

RESOLUCIÓN Nro.14-DIEDMIL-D-003

Luis Garzón Narváez
General de Ejército
JEFE DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS

CONSIDERANDO:

Que el Comando Conjunto de las Fuerzas Armadas, aprobó el Mapa Doctrinario, en sesión de COMACO del 29 de junio de 2011.

Que el Manual de Operaciones de Información ha sido elaborado por el I Curso de Operaciones de Información, la Dirección de Operaciones de Información, validado por el Comité Doctrinario y revisado por la Dirección de Educación y Doctrina Militar del Comando Conjunto de las Fuerzas Armadas.

Que el Manual de Operaciones de Información ha cumplido con todas las fases del proceso de elaboración, actualización y producción de la doctrina conjunta.

Que el Manual de Operaciones de Información constituye una normativa doctrinaria para las operaciones militares.

En ejercicio de la facultad que le confiere el literal g) del artículo 16 de la Ley Orgánica de la Defensa Nacional:

RESUELVE:

Art. 1. Expedir el **"MANUAL DE OPERACIONES DE INFORMACIÓN"**

Art. 2. Derogar todos los manuales que sobre la materia hayan sido publicados con anterioridad a la presente fecha.

Registre, publique y póngase en ejecución.

Dado, en el Comando Conjunto de las Fuerzas Armadas en Quito D.M., a los catorce días del mes de agosto de dos mil catorce.

Luis Garzón Narváez
General de Ejército
JEFE DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS

OPERACIONES DE INFORMACION

“El uso de las Operaciones de Información puede disipar una crisis y evitar la necesidad de pasar a un conflicto armado”

ÍNDICE

CONTENIDO **PÁGINA**
INTRODUCCIÓN……..…….……....1
OBJETIVO…...……...……2
ALCANCE…….……2

CAPÍTULO I

ÁMBITO DE LA INFORMACIÓN Y SU RELACIÓN CON LAS OPERACIONES MILITARES

A. GENERALIDADES……..3
B. MARCO CONCEPTUAL…….7
C. EL ÁMBITO DE LA INFORMACIÓN……....8
D. LAS OPERACIONES MILITARES……..12
E. LOS PRINCIPIOS DE LAS OPERACIONES DE INFORMACIÓN……..…….……...18
F. LA COMUNICACIÓN ESTRATÉGICA.…….....23
G. LA IMPORTANCIA DE LAS O.I EN LAS OPERACIONES MILITARES…..……...……..23

CAPÍTULO II

CAPACIDADES PRINCIPALES, DE APOYO Y RELACIONADAS DE LAS OPERACIONES DE INFORMACIÓN

A. CAPACIDADES PRINCIPALES DE LAS OPERACIONES DE LA INFORMACIÓN……....25
B. CAPACIDADES DE APOYO DE LAS OPERACIONES DE INFORMACIÓN…….……...40
C. CAPACIDADES RELACIONADAS DE LAS OPERACIONES DE INFORMACIÓN……..……45

CAPÍTULO III

APOYO DE INTELIGENCIA A LAS OPERACIONES DE INFORMACIÓN

A. GENERALIDADES..……...……...…….……46
B. EL APOYO DE INTELIGENCIA A LAS OPERACIONES DE INFORMACIÓN.....……46
C. EL APOYO DE INTELIGENCIA A LA PLANIFICACIÓN DE LAS O.I…….....50
D. CONSIDERACIONES DE INTELIGENCIA EN LA PLANIFICACIÓN DE LAS OPERACIONES DE INFORMACIÓN…….....51

CAPÍTULO IV

RESPONSABILIDADES Y RELACIONES DE MANDO

A. AUTORIDAD……...56
B. RESPONSABILIDADES…….…56

CAPÍTULO V

PLANIFICACIÓN Y COORDINACIÓN DE OPERACIONES DE INFORMACION

A. GENERALIDADES……..……....62
B. LA PLANIFICACIÓN DE LAS OPERACIONES DE INFORMACIÓN……...62
C. CONSIDERACIONES DE PLANIFICACIÓN DE LAS OPERACIONES DE INFORMACIÓN…….....63
D. LA INTENCIÓN DEL COMANDANTE Y LAS OPERACIONES DE INFORMACIÓN.……..63
E. RELACIÓN ENTRE LAS MEDIDAS DE RENDIMIENTO Y LAS MEDIDAS DE EFECTIVIDAD……..…..64

CAPÍTULO VI

LA EDUCACIÓN PARA OPERACIONES DE INFORMACIÓN

A. GENERALIDADES……..71
B. LA EDUCACIÓN DE LAS OPERACIONES DE INFORMACIÓN……..71
C. EL ADIESTRAMIENTO DE LAS OPERACIONES DE INFORMACIÓN……....72
D. LA PLANIFICACIÓN DE LAS O.I PARA EJERCICIOS CONJUNTOS……..74
E. LAS OPERACIONES DE INFORMACIÓN EN EL ENTRENAMIENTO CONJUNTO……....81

APÉNDICE A

A. INSTRUCCIONES ADMINISTRATIVAS……83

MANUAL DE OPERACIONES DE INFORMACIÓN

INTRODUCCIÓN

Las Operaciones de Información son esenciales para la ejecución exitosa de las operaciones militares. El objetivo clave de las Operaciones de Información es lograr y mantener la superioridad de la información.

Se describe a las Operaciones de Información como el empleo integrado de las capacidades principales, de apoyo y relacionadas que se desarrollan en los procesos de Operaciones de Información aplicables a las amenazas propias.

En el capítulo I se considera el ámbito de la información y su relación con las operaciones militares.

El capítulo II analiza las capacidades principales de las Operaciones de Información necesarias para planificar y ejecutar con éxito las Operaciones de Información, incluye las capacidades principales, las capacidades de apoyo y las capacidades relacionadas en un ambiente conjunto.

El capítulo III trata del apoyo de la Inteligencia a las Operaciones de Información, revelando la importancia de las labores de esta especialidad para la preparación, planificación y evaluación de las Operaciones de Información.

El capítulo IV designa las responsabilidades y las relaciones de mando en las Operaciones de Información.

El capítulo V analiza la planificación y coordinación de las Operaciones de Información.

En el capítulo VI se aborda la educación militar en la planificación, ejecución, evaluación y control de las Operaciones de Información.

OBJETIVO

Disponer de Doctrina Conjunta de Operaciones de Información, que permita a los oficiales, voluntarios, tripulantes, y aerotécnicos, planificar, coordinar y ejecutar Operaciones de Información, de manera eficaz y eficiente que permita el logro de los objetivos propuestos en apoyo a las operaciones militares.

ALCANCE

El presente manual está dirigido a los oficiales, voluntarios, aerotécnicos y tripulantes que requieran planificar y ejecutar Operaciones de Información en apoyo a las operaciones militares.

CAPÍTULO I

ÁMBITO DE LA INFORMACIÓN Y SU RELACIÓN CON LAS OPERACIONES MILITARES

CAPÍTULO I

ÁMBITO DE LA INFORMACIÓN Y SU RELACIÓN CON LAS OPERACIONES MILITARES

A. GENERALIDADES

Las Operaciones de Información son esenciales para la ejecución exitosa de las operaciones militares. Un objetivo clave de las Operaciones de Información es lograr y mantener la superioridad de información. Se describe a las Operaciones de Información como el empleo integrado de las capacidades principales, de apoyo y relacionadas que se desarrollan en los procesos de Operaciones de Información aplicables a las amenazas propias con lo que es coherente con los procesos de restructuración de las Fuerzas Armadas, y que se detallan a continuación:

1. Capacidades Principales:

    - Operaciones Psicológicas
    - Operaciones de Decepción y Engaño
    - Guerra Electrónica
    - Seguridad en las Operaciones
    - Operaciones del Ciberespacio

2. Capacidades de Apoyo:

    - Inteligencia para Operaciones de Información

3. Capacidades Relacionadas:

    - Comunicación social

El propósito de esta doctrina es suministrar al Comando Conjunto, los Comandantes y Estados Mayores de los Comandos Operacionales una guía para ayudarlos a

preparar, planificar, ejecutar y evaluar las Operaciones de Información en apoyo a las operaciones militares.

Los Comandantes de los Comandos Operacionales integran sus acciones, fuerza y capacidad militar en todas las operaciones adicionando como aspecto importante las capacidades de Operaciones de Información, con la finalidad de crear y/o mantener los efectos deseados y medibles sobre los líderes, las fuerzas (regulares o irregulares), la información, los sistemas de información, y otros auditorios; mientras se protege y defiende las acciones, información y sistemas de información propias.

El Comandante evalúa la naturaleza de la misión y desarrolla el propósito para las Operaciones de Información en todas las fases de una operación militar.

Proporciona la doctrina conjunta para las operaciones y el adiestramiento, emite directrices militares para ser usadas por las Fuerzas Armadas al elaborar sus respectivos planes.

B. MARCO CONCEPTUAL

1. Información

Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado del conocimiento del sujeto o sistema que recibe dicho mensaje.
La información está constituida por un grupo de datos ya supervisados y ordenados, que sirve para constituir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

2. Sistemas de Información

Toda infraestructura, organización, personal y componentes que recopilen, procesen, almacenen, transmitan, muestren, diseminen y actúen con información.

3. Operaciones de Información

Es el conjunto de acciones coordinadas que se realizan para influir en la toma de decisiones del adversario, en apoyo a la consecución de los objetivos propios, influyendo en su capacidad para explotar, proteger y contrarrestar las amenazas que trae el entorno de información, éstas son de naturaleza ofensiva, defensiva, y se apoyan en la inteligencia, y en los sistemas de mando y control.

4. Ciberespacio

Es un espacio virtual que "contiene" todos los recursos de información y comunicación disponibles en la red, donde los sujetos interactúan entre sí, a través de las nuevas tecnologías, las barreras físicas desaparecen, tiempo y espacio toman una nueva dimensión, y un individuo puede comunicarse con otros individuos en diferentes lugares del planeta al mismo tiempo. El ciberespacio se ha convertido en los últimos años en una parcela global que interactúa y/o afecta directamente también a los espacios marítimos, aéreos y espaciales.

5. Ciberdefensa

Constituye una iniciativa diseñada para ampliar los sistemas de defensa de los Estados y protegerlos de los nuevos riesgos emergentes en la sociedad de la información. Entre estos riesgos se encuentran la “guerra cibernética”, entendida como la utilización de

las debilidades de las redes informáticas que van desde el espionaje y la infiltración de los sistemas informáticos hasta la destrucción física de los recursos del oponente; y el “espionaje cibernético”, cuyo objetivo es obtener información confidencial circulante en ese medio. La Ciberdefensa es fundamental en este momento, en el que se han visto las enormes consecuencias que este tipo de ataques pueden generar a la seguridad del Estado.

6. Ciberseguridad

Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.

7. Superioridad de Información

El grado de dominio de información que permite la ejecución de las operaciones sin oposición. La ventaja operacional se deriva de la habilidad de recopilar, procesar y difundir un flujo continuo de información; mientras se explota o se le niega al adversario la habilidad de hacer lo mismo.

8. Sistemas de Control de Supervisión y Adquisición de Datos

Son el hardware y el software que controlan las plantas de energía, vías férreas, represas, sistemas de teléfonos y las redes eléctricas etc.

9. Enciclopedia Básica

Es la cantidad total de personas, organizaciones y sistemas que recopilan, procesan, difunden la información, o actúan sobre la misma. Son una compilación de instalaciones identificadas y áreas físicas de posible importancia como objetivos de un ataque. En estas instalaciones el adversario dispone de medios e información clave para ejercer el mando y control.

10. Capacidades Principales

Son los pilares fundamentales en que se sustentan las Operaciones de Información a través de Operaciones Psicológicas, Operaciones de Decepción y Engaño, Guerra Electrónica, Seguridad en las Operaciones y Operaciones de Ciberespacio.

11. Capacidades de Apoyo

Son las capacidades que soportan las Operaciones de Información incluyen la garantía de la información, la seguridad física, el ataque físico, la contrainteligencia. Estas están directa o indirectamente involucradas en el ámbito de la información y contribuyen a la eficacia de las Operaciones de Información, deben estar integradas y en coordinación con las capacidades principales: Operaciones Psicológicas, Operaciones de Decepción y Engaño, Guerra Electrónica, Seguridad en las Operaciones y Operaciones de Ciberespacio, pero

también pueden servir para otros propósitos más amplios.

12. Capacidades Relacionadas

Las capacidades que contribuyen a las Operaciones de Información y siempre deben ser coordinadas e integradas con las capacidades principales y capacidades de apoyo.

C. EL ÁMBITO DE LA INFORMACIÓN

El ámbito de la información en las Operaciones de Información incluirá la cantidad total de personas, organizaciones y sistemas que recopilan, procesan, difunden la información, o actúan sobre la misma. Entre los actores se incluye a los jefes, el personal en el nivel estratégico y operacional que adoptan decisiones, así como el personal, los sistemas informáticos y demás organizaciones y medios que materializan las Operaciones de Información. Los recursos incluyen los materiales y los sistemas que se emplean para recopilar, analizar, aplicar, o difundir la información. El ámbito de la información es donde los seres humanos y los sistemas automatizados observan, orientan, determinan la información, y actúan en base a la misma, y es por lo tanto el ambiente principal de la toma de decisiones incluyendo las tres dimensiones del campo de batalla y el ciberespacio; la firma, los informativos y lo cognitivo.

1. La Dimensión Física

La dimensión física está compuesta por los sistemas de mando y control, y las infraestructuras de apoyo que les permiten a las personas y organizaciones llevar a cabo operaciones a través de los dominios aéreo, terrestre, marítimo y espacial. Es también la dimensión donde están las plataformas físicas y las redes de comunicaciones que las conectan. Esto

incluye los medios de transmisión, infraestructura, tecnologías, grupos, y poblaciones. Comparativamente, los elementos de esta dimensión son los más fáciles de medir, y por consiguiente, la potencia de combate tradicionalmente se ha medido principalmente en esta dimensión.

2. La Dimensión Informativa

La dimensión informativa es donde se recopila, procesa, almacena, difunde, exhibe y protege la información. Esta dimensión donde se comunica el mando y control de la unidad militar moderna donde se expresa la inter unidad Comandante. Consiste en el contenido y el flujo de la información. Por consiguiente, es la dimensión informativa la que se debe proteger.

La dimensión informativa podría definirse como "el modo informativo que tiene por objeto la valoración, selección, clasificación y archivo para su posterior uso de textos y referencias sobre ideas, hechos, juicios y opiniones, con el fin de elaborar la información periodística y difundir información documental de base periodística."

Para caracterizar a la dimensión informativa, se han propuesto tres definiciones, correspondientes a sus tres dimensiones principales: (1) disciplina científica, (2) actividad profesional y (3) subsector económico.

3. La Dimensión Cognitiva

a) La dimensión cognitiva abarca la mente de la persona responsable de adoptar decisiones en el auditorio objetivo. Esta es la dimensión en la cual la gente piensa, percibe, visualiza y determina su forma de actuar. Es la más importante de las tres dimensiones. Esta dimensión también está afectada por las órdenes, el adiestramiento y otras motivaciones personales de un

Comandante. Se pueden perder batallas y campañas en la dimensión cognitiva. Factores tales como: el liderazgo, la moral, la cohesión de unidad, las emociones, el estado de ánimo, el nivel del adiestramiento, la experiencia, el conocimiento situacional; así como también la opinión pública, las percepciones, los medios de comunicación, la información pública y los rumores tienen influencia en esta dimensión.

b) Los avances en la tecnología han permitido que se recopile, procese, almacene, difunda, exhiba y proteja la información fuera del proceso cognitivo en cantidades y a velocidades que antes eran incomprensibles. Mientras la tecnología pone grandes cantidades de información a disposición del público en todo el mundo, los factores que afectan la percepción proporcionan el contexto que la gente emplea para traducir los datos en información y conocimientos.

c) Hay criterios que definen la calidad de la información en relación con su propósito, los criterios de calidad de información y los cambiantes propósitos requieren aplicaciones diferentes de estos criterios para clasificarlos como valiosos. Además, cada decisión depende de una ponderación diferente de los criterios de calidad de información para tomar la mejor decisión.

d) Se debe considerar la cantidad finita de tiempo y recursos disponibles para obtener información. Ya sea que se tomen las decisiones cognoscitivamente o de forma pre-programada en sistemas automatizados, la cantidad limitada de tiempo y recursos para mejorar la calidad de la información disponible dejan la toma de decisiones sujeta a la manipulación en el nivel

operacional. Además, hay aspectos reales vinculados con la obtención de información de calidad; es decir, información bien adaptada para su propósito, tales como los de adquirir, procesar, almacenar, transportar, y distribuir la información. El impacto, en conjunto, del éxito de las Operaciones de Información mejora la calidad de la información amiga, mientras que degrada la calidad de la información del adversario, proporcionándole de esta manera a las fuerzas amigas la posibilidad de tomar decisiones más rápidas y exactas.

e) Hay actividades vinculadas en la obtención de información de calidad, es decir, información bien adaptada para su propósito, tales como los de adquirir, procesar, almacenar, transportar y distribuir la información. El impacto en conjunto del éxito de Operaciones de Información mejora la calidad de la información amiga, mientras que degrada la calidad de la información del adversario, proporcionándole de esta manera a las fuerzas propias la posibilidad de tomar decisiones más rápidas y exactas.

CRITERIO DE CALIDAD DE INFORMACIÓN
EXACTITUD Información que expresa la situación real.
PERTENENCIA Información que corresponde a la misión, tarea o situación inmediata.
OPORTUNIDAD Información que se encuentra disponible a tiempo para tomar las decisiones.
USABILIDAD Información que está en un formato y visualizaciones comunes y fáciles de comprender.
INTEGRIDAD Información que le proporciona a la persona responsable de adoptar decisiones todos los datos necesarios.
CONCISIÓN Información que tiene solamente el nivel del detalle requerido.
SEGURIDAD Información a la que se le ha proporcionado la protección suficiente cuando fuera necesario.

Figura 1 Criterios de calidad de información

D. LAS OPERACIONES MILITARES Y EL ÁMBITO DE LA INFORMACIÓN

La información es un recurso estratégico vital para la seguridad nacional, el dominio del ámbito de la información es una realidad que se extiende por todos los ámbitos de las Fuerzas Armadas. Las operaciones militares, en particular, están en función de muchas actividades simultáneas e integradas que, a su vez, dependen de la información y los sistemas de información, los cuales se deben proteger.

En las operaciones militares modernas, los Comandantes se enfrentan a una variedad de desafíos de información. Los cambios técnicos incluyen el establecimiento y el mantenimiento de la conectividad, particularmente en los lugares austeros y apartados. Los desafíos operacionales incluyen la complejidad del combate moderno contra

adversarios con capacidades de información en crecimiento. Por ejemplo, sin considerar su tamaño, los adversarios, incluyendo los grupos terroristas, pueden contrarrestar los esfuerzos a través de las campañas de propaganda, o desarrollar, comprar, o descargar de Internet herramientas y técnicas que les permitan atacar la información y los sistemas de información, lo cual puede tener como resultado impactos concretos sobre los esfuerzos diplomáticos, económicos o militares. El ámbito de la información global y sus tecnologías asociadas se encuentran potencialmente al alcance de todos y por consiguiente los Comandantes, enfrentan otro desafío. El adversario tiene la capacidad de transmitir información, coordinar, intercambiar ideas, y sincronizar sus acciones al instante.

El Comandante visualiza, planifica y ejecuta las operaciones; las Operaciones de Información son una parte integral que apoya a la planificación y ejecución de dichas operaciones. La intención del Comandante, que en el caso de Fuerzas Armadas ecuatorianas es el concepto estratégico, el que debe especificar la visualización de los efectos deseados a ser conseguidos con las Operaciones de Información y demás operaciones para que el Estado Mayor desarrolle los objetivos de las Operaciones de Información. El Comandante no sólo debe poder visualizar los efectos deseados a conseguir con las Operaciones de Información, sino que también debe comprender mientras el adversario se esfuerza por lograr la superioridad de información. Estos efectos pueden variar en base a los objetivos de la misión, desde la planificación en tiempo de paz hasta cambiar la actitud de un Comandante adversario en combate. El papel de los militares y el efecto final deseado dependen de la naturaleza del conflicto. Si se está realizando una misión de asistencia humanitaria, entonces la generación de la buena voluntad por los servicios prestados y la partida con una impresión favorable hacia las actividades. La intención del

Comandante debe incluir el concepto de cómo ayudarán estos efectos a lograr los objetivos de la Fuerza.
Las unidades militares operan en un ámbito de la información de contenido y tiempo constantemente cambiantes. Esta evolución añade otra capa de complejidad al desafío de planificar y ejecutar las operaciones militares en un momento y/o área específica. La continuidad de factores a largo, mediano y corto plazo le dan forma al ámbito de la información para el cual se planifican las operaciones militares y en el que tales operaciones se ejecutan. Los Comandantes y jefes de Operaciones de Información deben estar preparados para adaptar o modificar los planes de las Operaciones de Información para lograr los efectos de las Operaciones de Información que deseen conseguir y deberá tener presente los siguientes factores:

1. Factores a Largo Plazo

Los factores a largo plazo que pueden dar forma al ámbito de la información incluyen las diversas maneras en las cuales los seres humanos:

- Se organizan (estados naciones, tribus, familias, etc.).
- Se gobiernan.
- Interactúan como grupos (la cultura, la sociología, la religión, etc.).
- Reciben influencia regional (la estabilidad, las alianzas, las relaciones económicas, etc.).
- Avanzan tecnológicamente.

2. Factores a Mediano Plazo

Los factores a mediano plazo podrían incluir los factores de riesgo y las amenazas comunes, el ascenso y caída de los líderes, la competencia entre grupos por recursos u objetivos, la incorporación de tecnologías específicas en la infraestructura de la información; y el empleo de recursos por parte de las

organizaciones para aprovechar la tecnología e infraestructura de la información.

3. Factores a Corto Plazo

Los factores a corto plazo podrían incluir el tiempo atmosférico; la disponibilidad de recursos limitados para soportar o emplear tecnologías de la información específicas; y la posibilidad de extender/mantener sensores e infraestructura de la información portátil a la ubicación específica de las operaciones militares distantes. La universalidad del ámbito de la información en las actividades humanas combinada con la velocidad y el poder de procesamiento de las tecnologías de información y comunicaciones modernas aumentan y complican los esfuerzos militares para organizar, adiestrar, equipar, planificar y operar. Actualmente, la tecnología ha abierto el camino a un grado de control siempre en aumento.

Las fuerzas llevan a cabo sus misiones en un ámbito de la información cada vez más complejo. Para que tengan éxito, es necesario que las fuerzas adquieran y mantengan la superioridad de información. Se describe a la superioridad de información como la ventaja estratégica y operacional que se obtiene mediante la habilidad de recopilar, procesar, y difundir un flujo ininterrumpido de información mientras se le explota o se le niega la posibilidad a un adversario de hacer lo mismo. Para obtener la superioridad de información se deberá tomar en cuenta lo siguiente:

a) Las fuerzas que poseen mejor información y que usan esa información para adquirir conocimiento de manera más eficaz tienen una ventaja muy importante sobre sus adversarios. Un Comandante que obtiene esta ventaja puede emplearla para cumplir misiones afectando las percepciones, las actitudes, las decisiones y las

acciones. Sin embargo, la superioridad de información no es estática; durante las operaciones todos los bandos intentan continuamente asegurar sus propias ventajas y negarles la información útil a los adversarios. Las ventajas operativas de la superioridad de información pueden tomar varias formas, que van desde la habilidad de crear una situación operacional conjunta hasta la habilidad de retrasar la decisión de un adversario de empeñar refuerzos en combate.

b) El reconocimiento de la superioridad de información puede ser difícil de conseguir sobre ciertos adversarios, pero sus ventajas son importantes. Cuando existe, la información que los Comandantes tienen a su disposición les permite visualizar la situación con exactitud, anticiparse a los eventos, y tomar las decisiones apropiadas y en el momento oportuno, y de manera más eficaz que los responsables de adoptar decisiones del adversario. En esencia, la superioridad de información aumenta la libertad de acción de los Comandantes y permite que pongan en práctica las decisiones y conserven la iniciativa, mientras se mantienen dentro del ciclo de decisión del adversario. Sin embargo, los Comandantes reconocen que sin Operaciones de Información ininterrumpidas diseñadas para lograr y mantener la superioridad de información, los adversarios pueden contrarrestar esas ventajas y, posiblemente, lograr la superioridad de información ellos mismos. Los Comandantes pueden conseguir la superioridad de información manteniendo la comprensión situacional exacta, mientras controlan o afectan las percepciones de los adversarios. Cuanto más un Comandante pueda plasmar esta disparidad, mayor será su ventaja.

Los adversarios de información potenciales pueden tomar muchas formas, países tradicionalmente hostiles que desean obtener información sobre las capacidades e intenciones militares, piratas informáticos maliciosos que desean hacerles daño; los terroristas; y los competidores económicos, sólo por mencionar algunos. Las técnicas de ataque de la información del adversario son numerosas. Algunas se pueden evitar mediante la aplicación constante de la encriptación, los cortafuegos y otras técnicas de seguridad de redes. Otras, son considerablemente más difíciles de contrarrestar. Las técnicas de amenaza a la información incluyen: el engaño, el ataque electrónico, el ataque de las redes de computadoras, la propaganda, las operaciones psicológicas y las operaciones de apoyo de inteligencia electrónica, pero no se limitan a ellos.

Con el flujo libre de información presente en todos los teatros de operaciones, como en la televisión, la telefonía e Internet, pronto pueden aparecer mensajes en conflicto para neutralizar los efectos previstos. Por consiguiente, se hace imperativa la sincronización y coordinación ininterrumpida entre las Operaciones de Información, los asuntos públicos, la diplomacia pública y nuestros aliados, y ayudarán a garantizar que los temas de información empleados durante las operaciones que involucren a poblaciones neutrales o amigas se mantengan constantes.

Consideraciones legales en las Operaciones de Información pueden involucrar asuntos legales y políticos complejos que requieren una evaluación cuidadosa. Más allá del acatamiento estricto de las cuestiones legales, las actividades militares en el ámbito de la información como en los dominios físicos, son llevadas a cabo como un asunto de política y valores sociales sobre la base del respeto por los

derechos humanos fundamentales. A las fuerzas que operen físicamente desde bases o ubicaciones de ultramar o dentro de los límites, se les exige por ley y política que actúen de conformidad con la ley de conflictos armados.

E. LOS PRINCIPIOS DE LAS OPERACIONES DE INFORMACIÓN

1. El éxito en las operaciones militares depende de la recopilación e integración de la información esencial mientras se le niega al adversario y a otros. Las Operaciones de Información abarcan la planificación, coordinación, y sincronización del empleo de las capacidades actuales para afectar o defender deliberadamente el ámbito de la información para lograr los objetivos del Comandante.

2. Las Operaciones de Información tienen que ver principalmente con influir en las decisiones y los procesos de toma de decisiones, mientras al mismo tiempo se defiende los procesos de toma de decisiones amigos. Los mecanismos principales que se emplean para afectar el ámbito de la información incluyen: la influencia, la interrupción, la corrupción o la usurpación.

3. La posibilidad de las Operaciones de Información de influenciar y defender la toma de decisiones está basada en cinco suposiciones fundamentales. Aunque cada una de estas suposiciones es un factor habilitante importante para las Operaciones de Información, no todas ellas serán verdaderas para cada operación necesariamente. Para cualquier operación específica donde una o más de estas suposiciones no se cumplan, la evaluación de riesgo proporcionada al Comandante sería ajustada en consecuencia. Las suposiciones fundamentales a considerar son las siguientes:

a) En general, la calidad de la información que se considera valiosa para los responsables de adoptar decisiones humanas y automatizadas es universal. Sin embargo, la importancia relativa de cada criterio de calidad de información podría variar en base a las influencias de la geografía, la lengua, la cultura, la religión, la organización, la experiencia, o la personalidad.

b) Se toman las decisiones sobre la base de la información disponible en el momento.

c) Es posible, con recursos finitos, comprender los aspectos relevantes del ámbito de la información para incluir los procesos que emplean las personas responsables de adoptar las decisiones para tomar las mismas.

d) Es posible influenciar el ámbito de la información en el cual actúan los responsables de tomar decisiones específicas, a través de los medios psicológicos y electrónicos o físicos.

e) Es posible medir la efectividad de las acciones de las Operaciones de Información en relación a un objetivo operacional.

4. Dado que la actividad humana tiene lugar en el ámbito de la información está potencialmente sujeta a las Operaciones de Información. Sin embargo, sólo los aspectos psicológicos, electrónicos y físicos críticos del ámbito de la información relacionados con la misión deben ser directa o indirectamente el objetivo de las Operaciones de Información.

5. Las capacidades de las Operaciones de Información pueden causar efectos y lograr objetivos en todos los niveles del conflicto, y por todo el espectro de las

operaciones militares. La naturaleza del ámbito de la información moderna complica la identificación de los límites entre estos niveles. Por lo tanto, en todos los niveles, las actividades de información, incluyendo las Operaciones de Información, deben ser compatibles con la política de seguridad y objetivos estratégicos nacionales.

6. Dado que las Operaciones de Información se llevan a cabo en todo el espectro de las operaciones militares y pueden realizar importantes contribuciones antes de que comiencen las operaciones principales, se debe preparar y evaluar el ambiente de las Operaciones de Información a través de una variedad de actividades de enfrentamiento y de inteligencia, todas diseñadas para hacer más eficaces a las Operaciones de Información. Además de tener impacto sobre el ambiente antes del inicio de las operaciones militares, las Operaciones de Información son esenciales para las operaciones posteriores al combate; por lo tanto, la integración, la planificación, el empleo y la evaluación de las Operaciones de Información principales, de apoyo y relacionadas son vitales para asegurar una transición rápida a un ambiente de paz.

7. El objetivo estratégico final de las Operaciones de Información es potenciar las operaciones militares y contribuir con el concepto estratégico del Comandante del más alto nivel, disuadir a un adversario potencial o real o a otro de que inicien acciones que amenacen los intereses nacionales. Además, las acciones de Operaciones de Información llevadas a cabo mediante departamentos del ámbito de la información global controladas por civiles o que puedan causar reacciones no intencionales como asuntos políticos y legales, para lo cual se debe considerar lo siguiente:

El centro de atención de las Operaciones de Información está en la persona responsable de tomar las decisiones y en el ámbito de la información con la finalidad de influenciar los procesos de toma de decisiones y de pensamiento, el conocimiento y la comprensión situacional. Las Operaciones de Información pueden influenciar los datos, la información y el conocimiento de tres maneras básicas:

a) Iniciando acciones psicológicas, electrónicas o físicas específicas que agregan, modifican o retiran información del ambiente de diferentes personas o grupos responsables de la toma de decisiones.

b) Iniciando acciones para influenciar la infraestructura que recopila, comunica, procesa y/o almacena información en apoyo de los responsables de la toma de decisiones.

c) Influyendo en la manera en que la gente recibe, procesa, interpreta y usa los datos, la información y los conocimientos.

8. Todas las capacidades de las Operaciones de Información se pueden emplear en todo tipo de operaciones. Los Comandantes emplean las capacidades de las Operaciones de Información en las operaciones militares de manera simultánea para cumplir la misión, incrementar la efectividad de su fuerza, y proteger sus organizaciones y sistemas.

   La integración total de las capacidades de las Operaciones de Información para las operaciones exige que los planificadores traten a las Operaciones de Información como una sola función. Los Comandantes pueden emplear las capacidades de las Operaciones de Información para lograr lo siguiente:

a) **Destruir.** Dañar un sistema o entidad de manera tal que no pueda desempeñar ninguna función o ser restaurado a una condición utilizable, sin ser reconstruido completamente.

b) **Desorganizar.** Dañar o interrumpir el flujo de la información.

c) **Debilitar.** Reducir la efectividad o eficiencia de los sistemas de C3I2 o de comunicaciones y los esfuerzos o medios de recopilación de información del adversario. Las Operaciones de Información también pueden debilitar la moral de una unidad, reducir la valía o el valor del objetivo o reducir la calidad de las decisiones y las acciones del adversario.

d) **Negar.** Impedirle al adversario tener acceso a información, sistemas y servicios críticos y usar los mismos.

e) **Engañar.** Hacer que una persona crea algo que no es cierto. Las Operaciones de Decepción y Engaño buscan afectar a los encargados de la toma de decisiones.

f) **Explotar.** Lograr el acceso a los sistemas de C3I2 del adversario.

g) **Influenciar.** Hacer que otros actúen de forma favorable a las fuerzas propias.

h) **Proteger.** Iniciar acciones para protegerse contra el espionaje o la captura de equipo e información confidencial.

i) **Detectar.** Descubrir o discernir la existencia, presencia o realización de una intrusión en los sistemas de información.

j) Restituir. Devolver los sistemas de información y la información a su estado original.

k) Responder. Reaccionar rápidamente frente a un ataque o intrusión de operaciones información del adversario o de otros.

F. LA COMUNICACIÓN ESTRATÉGICA

La comunicación estratégica integra los esfuerzos del Estado que se encuentra en comprender y comprometer los auditorios objetivos con la finalidad de crear, fortalecer, o mantener las condiciones favorables para el avance de los intereses, políticas y objetivos del Estado mediante el uso de programas, planes, temas, mensajes y productos sincronizados con las acciones de todos los elementos del poder nacional.

Los esfuerzos de las Fuerzas Armadas deben ser parte de un enfoque de todo el gobierno para desarrollar e implementar una capacidad de comunicación estratégica más vigorosa.

G. LA IMPORTANCIA DE LAS OPERACIONES DE INFORMACIÓN EN LAS OPERACIONES MILITARES.

La historia indica que la velocidad y la exactitud de la información disponible para los Comandantes son los factores significativos al determinar el resultado en el campo de batalla. Las Operaciones de Información buscan la exactitud y la oportunidad de la información que los Comandantes necesitan defender nuestros sistemas de la explotación por parte de los adversarios, las O.I se emplea para denegar a los adversarios el acceso a su información de mando y control sobre sus sistemas de explotación.

Cada vez más los adversarios están explorando y evaluando las acciones de Operaciones de Información como una guerra asimétrica que se puede usar para frustrar los objetivos militares planteados, que son altamente dependientes de los sistemas de información. Esto requiere que los militares empleen tácticas, técnicas y procedimientos ofensivos y defensivos para impedir que se ataque a nuestras fuerzas y sistemas con éxito.

Las fuerzas que poseen mayor información y que usan esa información para adquirir conocimiento de manera más eficaz tienen una ventaja muy importante sobre sus adversarios. Un Comandante que obtiene esta ventaja puede emplearla para cumplir misiones afectando las percepciones, las actitudes, las decisiones y las acciones. Sin embargo la superioridad de información no es estática; durante las operaciones todos intentan continuamente asegurar sus propias ventajas y negarles la información útil a los adversarios. Las ventajas de la superioridad de información pueden tomar varias formas, que van desde la habilidad de crear una situación operativa conjunta hasta la habilidad de retrasar la decisión de un adversario de empeñar refuerzos.

CAPÍTULO II

CAPACIDADES PRINCIPALES DE APOYO Y RELACIONADAS DE LAS OPERACIONES MILITARES

GUERRA ELECTRÓNICA

OPERACIONES DE DECEPCIÓN Y ENGAÑO

SEGURIDAD EN LAS OPERACIONES

OPSIC

INTELIGENCIA

COMUNICACION SOCIAL

CAPÍTULO II

CAPACIDADES PRINCIPALES, DE APOYO Y RELACIONADAS DE LAS OPERACIONES DE INFORMACIÓN.

Las Operaciones de Información, considerando que es una disciplina en evolución del mundo militar y conociendo que son las acciones que afectan la información del adversario y sus sistemas de información, protegiendo los propios; se requiere coordinar y sincronizar el empleo de las capacidades principales, de apoyo y relacionadas para el apoyo a las operaciones militares.

A. CAPACIDADES PRINCIPALES DE LAS OPERACIONES DE LA INFORMACIÓN.

Las capacidades principales son: Operaciones Psicológicas, Operaciones de Decepción y Engaño, Guerra Electrónica, Seguridad en las Operaciones; y Operaciones de Ciberespacio de las cinco, operaciones psicológicas y la guerra electrónica han tenido una participación importante en las operaciones militares en conflicto pasados. Hoy en día contamos con Operaciones de Decepción y Engaño, la Seguridad en las Operaciones y la Seguridad del Ciberespacio.

1. OPERACIONES PSICOLÓGICAS

Las Operaciones Psicológicas son actividades militares, económicas, políticas y psicosociales planificadas, que incluyen la “Acción Psicológica” y la “Guerra Psicológica”, para ser utilizadas tanto en tiempo de paz como en la guerra, dirigidas hacia auditorios objetivos” adversarios, amigos neutrales” con el propósito de influenciar en sus actividades y comportamientos, necesarios para el logro de los objetivos políticos y militares.

Las Operaciones Psicológicas tienen un papel importante en el logro de los objetivos de las Operaciones de Información en apoyo a una operación militar. En el ámbito de la información actual, incluso las Operaciones Psicológicas llevadas a cabo en el nivel táctico pueden tener efectos estratégicos. Por lo tanto, las Operaciones Psicológicas tienen un proceso de aprobación. Esto es especialmente importante en las primeras etapas de una operación dado el tiempo que se requiere para desarrollar, diseñar, producir, distribuir, difundir y evaluar los productos y acciones de las Operaciones Psicológicas. Todas las OPSIC se llevan a cabo con la ejecución de campañas, programas y actividades del área coordinadas de forma integral y aprobada por la Dirección de Operaciones de Información del CC.FF.AA.

El Director de Operaciones de Información debe iniciar la planificación, tan pronto como sea posible, para garantizar la ejecución de las operaciones psicológicas en apoyo de las operaciones militares. Los jefes de los departamentos de Operaciones de Información deben tener programas y actividades de operaciones psicológicas aprobados, sus recursos pueden ser de un valor esencial para los jefes de los departamentos de Operaciones de Información de los Comandos Operacionales, las operaciones psicológicas deben coordinar con inteligencia, seguridad de las operaciones, operaciones de decepción y engaño, guerra electrónica; para asegurar la coordinación y control del logro de los objetivos establecidos en la planificación.

Debe haber una cooperación y coordinación estrecha entre el centro de coordinación de Operaciones de Información y Comunicación Social para mantener la credibilidad de sus auditorios respectivos, que es el propósito de Operaciones de Información.

Los esfuerzos de operaciones psicológicas son más eficaces cuando se incluye a personal con una comprensión cabal de la lengua y la cultura del auditorio objetivo en la revisión de los materiales y mensajes de las operaciones psicológicas. A medida que evoluciona el ámbito de la información, la difusión de los productos de OPSIC va en aumento desde el material impreso y la radiodifusión tradicional hasta el uso más sofisticado de las telecomunicaciones. La efectividad de las OPSIC se aumenta mediante la sincronización y la coordinación de las capacidades principales, de apoyo y relacionadas de las Operaciones de Información.

Se planificarán las Acciones Psicológicas y Guerra Psicológica para el apoyo de la campaña.

a) Acción Psicológica

Son actividades planificadas para alcanzar, del auditorio objetivo amigo y neutral, el apoyo a las operaciones militares; estas se realizan para aumentar la voluntad de lucha y elevar la moral de las propias tropas.

b) Guerra Psicológica

Es el uso planificado de la propaganda y otras técnicas, dirigido a auditorios objetivos adversarios con la finalidad de dividir, desprestigiar a los mandos políticos y militares, restar la voluntad de lucha y motivar la deserción de sus tropas.

2. OPERACIONES DE DECEPCIÓN Y ENGAÑO

Operaciones de decepción y engaño se pueden planificar a nivel estratégico y se ejecutan hasta en el nivel táctico.

Otra operación importante que contribuirá a la seguridad de las operaciones militares, es sin duda la decepción y engaño. Estas operaciones se describen como las acciones ejecutadas para engañar deliberadamente a los responsables de tomar decisiones adversarias respecto a las capacidades, las intenciones y las operaciones amigas, causando de este modo que el adversario realice las acciones específicas o deje de hacerlas, que contribuirán al logro del cumplimiento de la misión de las fuerzas propias, las operaciones de decepción y engaño tratan de propiciar el análisis incorrecto, provocando que el adversario llegue a deducciones falsas específicas y las operaciones sicológicas influenciarán en los auditorios objetivos. Para ser eficaz, una operación de decepción y engaño debe ser susceptible a las acciones de los sistemas adversarios de recopilación de información y ser considerada como creíble por el Comandante adversario.

Un enfoque razonable para la planificación de las operaciones de decepción y engaño es emplear un curso de acción que las fuerzas amigas puedan ejecutar y que la inteligencia adversaria pueda verificar. Sin embargo, los planificadores de las operaciones de decepción y engaño no deben caer en la trampa de atribuirle al adversario en determinadas actitudes, valores y reacciones que “reflejan la imagen” de probables acciones amigas en la misma situación. Por ejemplo suponer que el adversario responderá o actuará de una manera en particular sobre la base de cómo responderíamos ante la situación.

Hay prioridades siempre en conflicto por los recursos necesarios para el engaño y los recursos necesarios para la operación real. Por esta razón, el plan de engaño se debe desarrollar simultáneamente con el

plan verdadero, comenzando con la apreciación inicial del Comandante y del Estado Mayor, para asegurar los recursos apropiados para ambos. Para propiciar el análisis incorrecto por parte del adversario, generalmente es más efectivo y eficaz darle un propósito falso a la actividad verdadera que inventar una actividad falsa.

En las operaciones de decepción y engaño es importante el involucramiento de todos quienes van a efectuar la operación militar a todo nivel, ya que el peligro del engaño puede desenmascarar el plan verdadero. Esta necesidad de la planificación debe ser de acceso restringido mientras se garantiza la coordinación detallada, lo cual es el desafío mayor para los planificadores de las operaciones de decepción y engaño.

Las operaciones de decepción y engaño son fundamentales para el éxito de las Operaciones de Información, pero se requiere de un alto grado de coordinación con todos los elementos de las actividades de las fuerzas amigas en el ámbito de la información así como también con las actividades operativas. Cada una de las capacidades principales, de apoyo y relacionadas tiene un papel que desempeñar en el desarrollo de una operación de decepción y engaño exitosa y en el mantenimiento de su credibilidad en el tiempo.

3. GUERRA ELECTRÓNICA

Las Operaciones de Información capitalizan la creciente sofisticación, conectividad y confianza en la tecnología de la información y comunicación. Las Operaciones de Información se dirigen a alcanzar la superioridad de la información basado en los sistemas de información y las telecomunicaciones.

La tecnología de información y comunicación (TIC) es esencial dentro de las Operaciones de Información, porque son el conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética. Es por ello que se considera importante dentro de las Operaciones de Información como: las operaciones de redes informáticas y las telecomunicaciones.

Las operaciones de redes informáticas, junto con la guerra electrónica, se utilizan para atacar, engañar, degradar, interrumpir, denegar, explotar la infraestructura del adversario y defender la propia. En vista de que el enfoque es producir un efecto disuasivo, el ataque a una red informática representa el subcomponente más viable "generador de efectos".

Los adversarios dependen cada vez más de computadoras y redes informáticas con el fin de facilitar mando y control, transacciones que hacen posible el apoyo y la coordinación de medidas. El ataque contra las redes informáticas ofrece la posibilidad de ser un arma de interrupción masiva contra blancos estructurales, tanto militares como civiles.

La defensa de redes informáticas niega al adversario información crucial que podría facilitarle una evaluación acertada de las intenciones y capacidades propias. Estas operaciones por falta de información creíble, ocasionan que el adversario tome malas decisiones o posponga la toma de las mismas; así como negar información crítica sobre las intenciones y capacidades del adversario, ayudando a aumentar su incertidumbre, desestabilizar su ciclo de toma de

decisiones e incrementar, cada vez más, sus dudas, temor y confusión.

La explotación de las redes informáticas, al recopilar cualquier tipo de información importante del adversario, ayudará que esta información pueda ser utilizada dentro de la planificación de las Operaciones de Información para obtener una ventaja contra del adversario, se debe tener en cuenta también que la propagación de datos confidenciales a través de la red, puede comprometer a la nación a la que pertenece y en muchas ocasiones esta se ve comprometida frente a dichos ataques o también corre peligro de ser eliminada información vital.

a) Las Telecomunicaciones

Son las transmisiones, emisiones o recepciones de signos, señales, datos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de cables, medios ópticos, físicos u otros sistemas electromagnéticos. Los elementos que integran un sistema de telecomunicación son un transmisor, una línea o medio de transmisión y posiblemente, impuesto por el medio, un canal y finalmente un receptor. Las telecomunicaciones cubren todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de computadoras a nivel de enlace.

Las telecomunicaciones pueden ser punto a punto, punto a multipunto o teledifusión, que es una forma particular de punto a multipunto que funciona solamente desde el transmisor a los receptores, siendo su versión más popular la radiodifusión.

La Dirección de Telecomunicaciones del CC.FF.AA es responsable de planificar y emitir directrices en el ámbito de las telecomunicaciones de Fuerzas Armadas, por lo que es necesario una estrecha coordinación de las Operaciones de Información con las telecomunicaciones, debido a que a través de su Departamento de Planificación elabora la estrategia y direccionamiento concerniente a las telecomunicaciones de FF.AA., en su departamento de Gestión del Espectro, administra el uso de las frecuencias asignadas para la defensa con base en el Plan Militar de Frecuencias.

b) La Guerra Electrónica

Hace referencia a cualquier acción militar que involucre el uso y control del espectro electromagnético propio o adversario. Esta capacidad básica consta de tres subdivisiones: Ataque Electrónico, Protección Electrónica, y Apoyo de Guerra Electrónica.

La Guerra Electrónica tiene principios similares a las operaciones de redes por eso pueden ser soporte una de otra, considerando equipos informáticos y de comunicaciones, que vayan a ser utilizados o se deseen intervenir con la finalidad de lograr ventaja sobre el adversario según lo planificado por las Operaciones de Información.

1) El Ataque Electrónico

El ataque electrónico involucra el uso de la energía electromagnética dirigida a las armas anti radiación para atacar al personal, las instalaciones, o el equipo con el propósito de

debilitar, neutralizar o destruir la capacidad de combate del adversario.

2) La Protección Electrónica

La protección electrónica garantiza el uso amigo del espectro electromagnético y consiste en acciones asignadas, para buscar, interceptar, identificar y localizar fuentes de energía electromagnética irradiada con o sin intención con el propósito de reconocimiento de amenazas, localización de blancos, planificación, y la realización de operaciones futuras.

3) El Apoyo de Guerra Electrónica

El apoyo de guerra electrónica provee la información necesaria para las decisiones que involucran las operaciones de guerra electrónica y otras acciones tácticas, tales como la evitación de amenaza, la localización de blancos, y la autodirección de los sistemas de enlace. Se pueden emplear los datos de apoyo de guerra electrónica para producir inteligencia de señales, proporcionar localización de blancos para el ataque electrónico u otras formas de ataque.

La guerra electrónica contribuye al éxito de las Operaciones de Información empleando tácticas y técnicas ofensivas y defensivas en una variedad de combinaciones para explotar el empleo del espectro electromagnético por parte del adversario, mientras protege la libertad de acción amiga, dar seguridad en el espectro electromagnético e incrementar el potencial propio. La prevalencia creciente de la telefonía inalámbrica y el uso de las

computadoras amplía tanto la utilidad como la amenaza de la guerra electrónica, brindando oportunidades de explotar las vulnerabilidades electrónicas de un adversario y la necesidad de identificar y proteger las propias de una explotación similar.

A medida que el uso del espectro electromagnético se ha hecho universal en las operaciones militares, de la misma manera la guerra electrónica se ha visto involucrada en todos los aspectos de las Operaciones de Información. Todas las capacidades principales, de apoyo y relacionadas emplean la guerra electrónica directa o indirectamente.

La dirección de Operaciones de Información (G-6) debe coordinar con la dirección de Telecomunicaciones (G-5) el uso y apoyo de las telecomunicaciones.

El uso y empleo de Guerra Electrónica por parte de las Operaciones de Información es necesario coordinar con el Comandante operativo de Guerra Electrónica.

c) Las Operaciones de Redes Informáticas

Son una de las más recientes capacidades que se han desarrollado en apoyo de las operaciones militares y son el resultado del uso creciente de las computadoras conectadas en red, y de los sistemas de infraestructura de las tecnologías de información de apoyo por parte de las organizaciones militares y civiles. Las operaciones de redes informáticas, junto con la guerra electrónica se emplean para atacar, engañar, debilitar, trastornar, denegar, explotar la información enemiga y defender la información y

la infraestructura electrónica de las Fuerzas Armadas propias. Para el propósito de las operaciones militares, las operaciones de redes informáticas se dividen en: ataque de redes informáticas, defensa de redes informáticas y la explotación de las redes informáticas.

1) El Ataque de Redes Informáticas

El ataque de redes informáticas consiste en las acciones llevadas a cabo a través del uso de las redes informáticas para afectar, denegar, debilitar o destruir la información residente en las computadoras y redes del adversario.

2) La Defensa de Redes Informáticas

La defensa de redes informáticas involucran las acciones del uso de las redes informáticas para proteger, monitorear, analizar, detectar y responder a la actividad no autorizada dentro de los sistemas de información y redes.

Las acciones de la defensa de redes informáticas no solamente protegen a los sistemas propios del ataque del adversario externo, sino que también del uso y explotación en el ámbito interno que son una función necesaria en todas las operaciones militares.

3) La Explotación de las Redes Informáticas

La explotación de las redes informáticas permite que las operaciones de recopilación de inteligencia llevadas a cabo a través del uso de las redes de computadoras, recojan

datos de sistemas o redes de información del adversario.

La dependencia creciente de los grupos militares y adversarios de las computadoras y redes informáticas para proporcionar información de comando y control a sus fuerzas, refuerza la importancia de las operaciones de redes informáticas en los planes y actividades de las Operaciones de Información. A medida que se incremente la capacidad de las computadoras y la extensión de su empleo, continuarán desarrollándose nuevas vulnerabilidades y oportunidades. Esto brinda oportunidades de atacar y explotar las debilidades del sistema informático del adversario y la necesidad de identificar y proteger el propio de un ataque o explotación similar.

4. SEGURIDAD EN LAS OPERACIONES

La seguridad en las operaciones es un proceso de identificación de información esencial y posterior análisis de las acciones y otras actividades propias, con la finalidad de identificar qué información es necesaria que el adversario tenga conocimiento; negarle a quien toma las decisiones del adversario la información esencial de fuerzas propias y provocar que los responsables de la toma de decisiones del adversario no juzguen apropiadamente la relevancia de la información esencial obtenida, asegurando también el resto de la información.

Con la seguridad en las operaciones se logrará impedir detectar las verdaderas intenciones; negando al adversario la información necesaria para evaluar correctamente las capacidades e intenciones amigas.

En particular, esta capacidad complementa a una operación de decepción y engaño.

Además, las operaciones de seguridad pueden ocasionar que el adversario por falta de información creíble, tome inadecuadas decisiones.

Negar información crucial sobre las propias intenciones y capacidades al Comandante adversario, ayuda a aumentar su incertidumbre, desestabilizar su ciclo de toma de decisiones e incrementar, cada vez más, sus dudas, temor y confusión, lo que hace posible un efecto de disuasión.

En el caso de las capacidades de las Operaciones de Información que explotan las nuevas oportunidades y vulnerabilidades, como las de: guerra electrónica, la seguridad en operaciones es esencial para garantizar que las capacidades de las fuerzas propias no se vean comprometidas.

El proceso de identificar los elementos esenciales de la información de una fuerza amiga y tomar medidas para cubrirlos de la revelación a los adversarios es sólo una parte de un enfoque de defensivo para asegurar la información. Para ser eficaz, se debe complementar la seguridad en las operaciones con otras clases de seguridad. Los ejemplos de otros tipos de seguridad incluyen la seguridad física y el ataque físico y los programas de garantía de la información y la defensa de redes informáticas.

a) La Seguridad Física

Es la parte de la seguridad que se encarga de las medidas físicas diseñadas para proteger al personal, impedir el acceso no autorizado al equipo, las instalaciones, el material, y los

documentos, y a protegerlos contra el espionaje, sabotaje, daño, y robo.

El proceso de seguridad física incluye la determinación de las vulnerabilidades a amenazas conocidas, la aplicación de las técnicas y medidas de protección de disuasión, control y negación apropiada, y la respuesta a condiciones cambiantes.

De la misma manera en que la garantía de la información protege la información y los sistemas de información electrónicos, la seguridad física protege las instalaciones físicas que contienen la información y los sistemas de información. La seguridad física, a menudo, contribuye a la seguridad en las operaciones, especialmente en el caso de las operaciones de decepción y engaño, donde el peligro de esta actividad podría comprometer el plan verdadero.

Los planes de las Operaciones de Información podrían requerir recursos significativos de seguridad física y se deben poner en conocimiento de la Dirección de Operaciones, tan pronto como sea posible, para que sean considerados en el proceso de planificación.

b) Ataque Físico

Considerando que el ataque es fundamental para las operaciones militares, el ataque físico trastorna, daña o destruye los objetivos adversarios a través del poder destructivo, este también se puede emplear para crear o modificar las percepciones del adversario o llevar al mismo a utilizar ciertos sistemas de información explotables.

El ataque físico se puede emplear en apoyo de las Operaciones de Información como un medio para atacar los sistemas de comando y control que afecten la posibilidad del adversario de ejercer el mando y de influenciar en los auditorios objetivo. Las operaciones psicológicas se pueden emplear en apoyo del ataque físico para maximizar el efecto del ataque sobre la moral del adversario.

La integración y la sincronización de fuegos con las Operaciones de Información a través del proceso de localización de blancos son fundamentales para crear la sinergia necesaria entre las Operaciones de Información y las operaciones militares. Debido al rápido desarrollo de la ejecución de las operaciones en los diferentes teatros de operaciones, es crucial que la planificación y la ejecución tanto de las Operaciones de Información como de las operaciones sean llevadas a cabo simultáneamente, para producir en forma eficaz el plan de localización de blancos.

c) La Garantía de la Información

La garantía de la información se define como las medidas que protegen y defienden la información y los sistemas de información que aseguran su disponibilidad, integridad, autenticación y confidencialidad. La garantía de la información es necesaria para obtener y mantener la superioridad de información, y se caracteriza porque integra las capacidades de las personas, las operaciones y la tecnología para establecer una protección de niveles múltiples que garantice el cumplimiento de la misión.

La garantía de la información considera que se puede obtener el acceso a la información y a los sistemas de información desde dentro y fuera de las redes controladas por el Comando Conjunto y las fuerzas. En una organización conjunta, la garantía de la información es una responsabilidad de todos sus componentes.

La garantía de la información y todos los aspectos de las operaciones de redes informáticas están interrelacionados y dependen los unos de los otros para ser eficaces. Las Operaciones de Información dependen de la garantía de la información para proteger la infraestructura, garantizar su disponibilidad y disponer de información que permita influenciar al adversario. Al contrario, la garantía de la información depende de las Operaciones de Información que en forma coordinada con las capacidades de seguridad de las operaciones, protección electrónica, defensa de redes informáticas, y contra-inteligencia negará los esfuerzos de Operaciones de Información o de inteligencia del adversario.

B. CAPACIDADES DE APOYO DE LAS OPERACIONES DE INFORMACIÓN

Las capacidades que apoyan las Operaciones de Información incluyen la inteligencia para Operaciones de Información. Estas están directa o indirectamente involucradas en el ámbito de la información y contribuyen a su efectividad. Deben estar integradas y coordinadas con las capacidades principales, seguridad en las operaciones después del ataque físico, pero también sirven para otros propósitos más amplios.

Las Operaciones de Información son inteligencia intensiva en particular y, por lo tanto, es planificada con preparación, ejecución y evaluación exitosa de

Operaciones de Información exige inteligencia detallada y oportuna.

1. Inteligencia para Operaciones de Información.

Antes de que se pueda planificar las actividades militares en el ámbito de la información, se requiere el apoyo de inteligencia militar para recopilar y analizar el "estado" actual del ámbito dinámico de la información, y suministrarlo a los Comandantes y a sus Estados Mayores. Esto requiere inteligencia sobre partes relevantes de las propiedades físicas, informativas y cognitivas del ámbito de la información, que necesita la recopilación y el análisis de una gran variedad de información y la producción de productos de inteligencia.

a) Las propiedades informativas del ambiente de la información.

Las propiedades informativas del ámbito de la información incluyen los sistemas y redes donde se crean, procesan, manipulan, transmiten y comparte la información. Incluyen las propiedades relevantes para la recopilación, transmisión, procesamiento, almacenamiento, y visualización electrónica de la información. Estas propiedades pueden ser electrónicas o de humano a humano, o una combinación de ambas. Describen la infraestructura y las redes de comunicaciones formales e informales, las relaciones de parentesco y descendencia, las relaciones comerciales licitas e ilícitas, y las afiliaciones y contactos sociales que crean, procesan, manipulan, transmiten y comparten colectivamente. La información en un área de operaciones y entre los auditorios objetivos:

1) La especificación capacidad, configuración y uso de la infraestructura y las capacidades de la información.
2) El diseño técnico de la infraestructura de la información.
3) Las redes de contacto de humano a humano que se emplean para la transmisión (correo, líneas de soplones, buzones secretos, etc.)
4) Las redes sociales y comerciales que procesan y comparten la información e influencia (los vínculos de parentescos y ascendencia, los contactos sociales formales e informales, las afiliaciones comerciales licitas e ilícitas, y los riesgos de propiedad y transacciones, etc).
5) El contenido y contexto.
6) Las propiedades cognitivas del ambiente de la información.
7) Las propiedades cognitivas del ambiente de la información son los atributos sicológicos, culturales, conductuales; además atributos humanos que incluyen en la toma de decisiones, el flujo de la información, y la interpretación de la información por parte de las personas o grupos en cualquier ámbito de un estado u organización.
8) Los factores culturales y sociales que afectan las aptitudes y percepciones tales como: la lengua, la educación, la historia, la religión, los mitos, la experiencia personal y la estructura familiar.
9) La identidad de personas y grupos clave que afectan las actitudes y percepciones.
10) La identidad y el perfil sicológico de los responsables de adoptar decisiones clave, sus asesores, socios clave, y/o miembros de su familia que tengan influencia sobre ellos.
11) La credibilidad de las personas o grupos clave y la especificación de su esfera de influencia.

12) Las leyes, reglas y procedimientos relevantes para la información y la toma de decisiones, los proceso de toma de decisiones, la doctrina de empleo de capacidades, la oportunidad, y el contenido de la información.
13) Cómo piensa, perciben, planean, ejecutan y evalúan los líderes las consecuencias de sus resultados y acciones desde sus perspectivas.

Mientras la aptitud de estos tipos de propiedades del ámbito de la información ilustra la diversidad de los requerimientos de inteligencia de las Operaciones de Información, es importante advertir que las fuentes y los métodos múltiples pueden ser necesarios para recopilar las propiedades físicas, informativas y cognitivas de los objetivos de recopilación específicos para fusionar y analizar propiedades diferentes en apoyo de la planificación de las Operaciones de Información. Por ejemplo, si la planificación operacional requiere inteligencia sobre las emisoras de radio dentro de un país adversario, ese requerimiento puede incluir la cantidad y la ubicación de las instalaciones de radioemisión y transmisión (física), las especificaciones técnicas de cada estación (informativa), la identidad de los propietarios y el personal clave, y la credibilidad o popularidad de cada estación (cognitiva).

b) El apoyo de inteligencia a la planificación de las Operaciones de Información.

El apoyo de inteligencia es una parte esencial de la planificación de las Operaciones de Información. En particular el proceso de preparación de inteligencia conjunta del espacio de batalla (JIPB) proporciona una metodología valiosa para identificar las capacidades, las vulnerabilidades y los nudos críticos dentro del

ambiente de la información. La JP2-01.3, tácticas, técnicas y procedimientos conjuntos para la preparación de inteligencia conjunta del espacio de batalla, trata el apoyo de la JIPB a las Operaciones de Información. Un vistazo general secuencial del apoyo de inteligencia a la planificación de Operaciones de Información incluye acciones para:

1) Identificar el valor, el uso, el flujo de las vulnerabilidades de información del adversario relevantes para tipos específicos de toma de decisiones.
2) Identificar sistemas individuales y conjuntos de objetivos relevantes para la toma de decisiones del adversario especificado a otro auditorio objetivo.
3) Identificar los efectos apropiados deseados para los sistemas individuales y conjuntos de objetivos.
4) Pronosticar las consecuencias (los resultados relacionados que no tengan que ver con los objetivos) de las acciones identificadas.
5) Coordinar con el personal de planificación para establecer la prioridad de los requerimientos de inteligencia.
6) Ayudar en el desarrollo de los criterios de evaluación de las Operaciones de Información durante la planificación y luego asistir en el monitoreo y la evaluación de las Operaciones de Información durante su ejecución (que pueden extenderse antes y después de la ejecución de las operaciones).
7) Adaptar la metodología de evaluación /retroinformación a las operaciones específicas.
8) Valorar el resultado de las actividades/tareas de las Operaciones de Información ejecutadas.

9) Llevar a cabo la evaluación para las acciones de las Operaciones de Información relativas a los objetivos y la misión.

C. CAPACIDADES RELACIONADAS DE LAS OPERACIONES DE INFORMACIÓN

El sistema de Comunicación Social es la capacidad relacionada que contribuye a las Operaciones de Información, siempre debe ser coordinada e integrada con las capacidades principales y de apoyo.

1. Comunicación Social

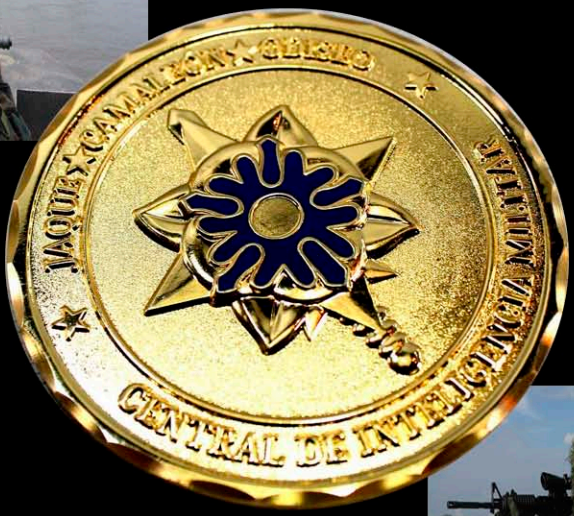
Es el proceso de intercambiar ideas y pensamientos, percepciones y significados entre un emisor y una fuente a través de un canal de comunicación directo o indirecto utilizando un elemento codificador como los símbolos del lenguaje.

También es un campo de estudio que explora principalmente las áreas de la información que puede ser percibida, transmitida e investigada la expresión de la información, de los medios de difusión masivos y las industrias culturales.

El oficial de enlace de Operaciones de Información debe coordinar las actividades, programas y la planificación realizada por Operaciones de Información G-6, con la finalidad de que sean difundidas a través del sistema de comunicación social de las Fuerzas a los diferentes auditorios objetivos, para apoyar las operaciones militares.

CAPÍTULO III

APOYO DE INTELIGENCIA A LAS OPERACIONES MILITARES



CAPÍTULO III

OPERACIONES DE INFORMACIÓN

A. GENERALIDADES

Como todos los demás aspectos de las operaciones conjuntas, las Operaciones de Información requieren un apoyo eficaz de inteligencia y por lo tanto la planificación, preparación, ejecución y evaluación exitosa de las Operaciones de Información exige inteligencia detallada y oportuna. La inteligencia respalda a la planificación y la ejecución de las Operaciones de Información en apoyo a las operaciones conjuntas.

B. EL APOYO DE INTELIGENCIA A LAS OPERACIONES DE INFORMACIÓN

Antes de que se puedan planificar las actividades militares en el ámbito de la información, se debe recopilar y analizar el estado actual del ámbito dinámico de la información, y suministrarlo a los Comandantes y a sus Estados Mayores. Esto requiere inteligencia sobre partes relevantes de las propiedades físicas, informativas y cognitivas del ámbito de la información, que necesita la recopilación y el análisis de toda la información para obtener Inteligencia para las Operaciones de Información como se menciona más adelante.

1. Naturaleza de los Requerimientos de Inteligencia de las Operaciones de Información

Es necesario realizar los requerimientos de inteligencia para comprender el proceso de toma de decisiones del adversario y determinar las capacidades, vulnerabilidades y susceptibilidades que deberán ser explotadas para lograr los objetivos propios estratégicos y operacionales, suministrarlos a los Comandantes y sus Estados Mayores con la

finalidad de ejecutar acciones de Operaciones de Información. Esto incluye las propiedades físicas, informativas y cognitivas relevantes del ámbito de la información; así como también la evaluación de las actividades de Operaciones de Información ejecutadas por el adversario.

a) Propiedades físicas del ámbito de la información incluyen a las personas, lugares, objetos y capacidades, infraestructura de la información, capacidades de información del adversario. Ejemplos:

    1) Las coordenadas geográficas de la infraestructura y de las capacidades de información del adversario.
    2) La organización de la infraestructura y capacidades, así como también la identificación de infraestructura de comunicación sobrante, y enlaces y nodos críticos.
    3) Los tipos, la cantidad, y la configuración de infraestructura y capacidades de la información (con marcas, modelos, y números específicos).
    4) Los procesos de planificación organizativa, decisión, y ejecución.
    5) El mecanismo de inteligencia y contrainteligencia del adversario para lograr la percepción, información y el conocimiento del campo de batalla.
    6) Las capacidades de ataque, defensa, y explotación del sistema informático del adversario.

b) Las propiedades informativas del ámbito de la información constituyen los sistemas y redes donde se crea, procesa, manipula, transmite y comparte la información, las propiedades

relevantes para la recopilación, transmisión, procesamiento, almacenamiento, y visualización electrónica de la información. Estas propiedades pueden ser electrónicas, humanas o una combinación de ambas. Describen la infraestructura y las redes de comunicaciones formales e informales lícitas e ilícitas, las afiliaciones y contactos sociales que crean, procesan, manipulan, transmiten y comparten colectivamente la información en una área de operaciones y entre los auditorios objetivos. Los ejemplos de propiedades informativas incluyen:

1) La especificación, capacidad, configuración, uso de los medios y las capacidades de la información.
2) El diseño técnico de los medios de la información.
3) Los contactos de persona a persona que se emplean para la transmisión de la información (correos, líneas dedicadas, buzones secretos, etc.).
4) Las redes sociales y comerciales que procesan y comparten información e influencia (los contactos sociales formales e informales, lícitas e ilícitas y los registros de propiedad y transacciones, etc.).
5) El contenido y contexto de la información.

c) Las propiedades cognitivas del ámbito de la información son los atributos psicológicos, culturales, conductuales y demás atributos humanos que influyen en la toma de decisiones, el flujo de la información, y la interpretación de la información por parte de las personas y/o grupos en cualquier ámbito en un estado u organización.

Las propiedades cognitivas pueden incluir:

1) Los factores culturales y sociales que afectan las actitudes y percepciones tales como: la lengua, la educación, la historia, la religión, los mitos, la experiencia personal y la estructura familiar.
2) La identidad de personas y grupos clave que afectan las actitudes y percepciones de una persona y/o grupo de personas.
3) La identidad y el perfil psicológico de los responsables de tomar decisiones claves, de sus asesores, socios claves, y/o miembros familiares que tengan influencia sobre ellos.
4) La credibilidad de las personas y/o grupos claves y la relación con su círculo de influencia.
5) Las leyes, reglas y procedimientos de información y toma de decisiones, la doctrina de empleo de sus capacidades, y de la información obtenida.
6) Cómo piensan, perciben, planifican, ejecutan y evalúan los líderes los resultados y las acciones obtenidas desde sus perspectivas.

2. Fuentes y Métodos para Recopilar las Propiedades

Mientras la amplitud de estos tipos de propiedades del ámbito de la información ilustra la diversidad de los requerimientos de inteligencia de las Operaciones de Información, es importante advertir que las fuentes y los métodos múltiples pueden ser necesarios para recopilar las propiedades físicas, informativas y cognitivas de los objetivos de recopilación específicos para fusionar y analizar propiedades diferentes en apoyo de la planificación de las Operaciones de Información; por ejemplo, si la planificación operacional requiere inteligencia sobre las emisoras de radio dentro de un país adversario, ese

requerimiento puede incluir la cantidad y la ubicación de las instalaciones de radioemisión y transmisión (física), las especificaciones técnicas de cada estación (informativa), la identidad de los propietarios y el personal clave, y la credibilidad o popularidad de cada estación (cognitiva).

C. EL APOYO DE INTELIGENCIA A LA PLANIFICACIÓN DE LAS OPERACIONES DE INFORMACIÓN

El apoyo de inteligencia es una parte esencial para la planificación de las Operaciones de Información, siendo que identifica las capacidades, las vulnerabilidades y los puntos críticos dentro del ámbito de la información. Las tácticas, técnicas y procedimientos para la Preparación de Inteligencia en el Campo de Batalla es el apoyo para la planificación de las Operaciones de Información incluyendo acciones para:

1. Identificar el valor, el uso, el flujo y las vulnerabilidades de información del adversario para la toma de decisiones.
2. Identificar sistemas individuales y conjuntos de objetivos relevantes para la toma de decisiones del adversario.
3. Identificar los efectos apropiados deseados para los sistemas individuales y conjuntos de objetivos.
4. Pronosticar las consecuencias (los resultados relacionados que no tengan que ver con los objetivos) de las acciones realizadas por grupos adversarios.
5. Coordinar con el personal de planificación para establecer la prioridad de los requerimientos de inteligencia.
6. Ayudar en el desarrollo de los criterios de evaluación de las Operaciones de Información durante la planificación y luego asistir en el monitoreo y la evaluación de las Operaciones de Información durante su ejecución (que puede extenderse antes y

después de la ejecución de las operaciones convencionales).

7. Adaptar las metodologías de evaluación a las operaciones específicas.
8. Valorar el resultado de las actividades y tareas de las Operaciones de Información ejecutadas.

D. CONSIDERACIONES DE INTELIGENCIA EN LA PLANIFICACIÓN DE LAS OPERACIONES DE INFORMACIÓN.

1. El impacto de la información sobre el apoyo de inteligencia y la naturaleza de la información tiene implicaciones profundas para el apoyo de inteligencia a las Operaciones de Información. Los miembros de inteligencia y operaciones deben comprender estas implicaciones para solicitar y suministrar apoyo de inteligencia a las Operaciones de Información de manera eficiente. Debemos considerar lo siguiente en el campo de la Inteligencia en la planificación de las Operaciones de Información.

2. Los recursos de inteligencia son limitados: los requerimientos de recopilación de información son casi limitados, especialmente para muchas clases de Operaciones de Información. Los Comandantes y sus direcciones de operaciones e inteligencia deben trabajar en conjunto para identificar los requerimientos de inteligencia para las Operaciones de Información y garantizar que se dé la prioridad lo suficientemente alta a estas solicitudes del Comandante en lo referente a Operaciones de Información.

3. Las actividades de recopilación están limitadas legalmente: la naturaleza del ámbito de la información complica el acatamiento de las limitaciones y restricciones legales. Por lo tanto, los organismos de inteligencia deben implementar métodos técnicos y de procedimiento para garantizar el acatamiento de la

ley. Además, se puede complementar la inteligencia con la información que proveen legalmente la ejecución de la ley u otras fuentes.

Especialmente en el área de las operaciones de redes informáticas, donde la aplicación de leyes nacionales e internacionales diferentes puede ser poco clara, es esencial la coordinación estrecha entre los organismos operacionales, legales y de ejecución de la ley.

4. La inteligencia de las Operaciones de Información a menudo requiere plazos de procesamiento largos. La inteligencia necesaria para influenciar las decisiones del adversario, a menudo, requiere que se dispongan y empleen con el tiempo fuentes y métodos específicos para recopilar la información necesaria y realizar los análisis que requiere la planificación de las Operaciones de Información. Los Comandantes y sus Estados Mayores, incluyendo los planificadores de Operaciones de Información, deben ser conscientes del tiempo de procesamiento necesario para desarrollar inteligencia, tanto para la planificación inicial como para el procesamiento y análisis de la información durante las operaciones. Para hacer frente a estos tiempos de procesamiento largos, el Comandante debe proporcionar una guía inicial detallada al Estado Mayor durante los procesos de recepción y análisis de la misión.

5. El ámbito de la información es dinámico: el ámbito de la información cambia con el tiempo de acuerdo a distintos factores. Los cambios físicos pueden tener lugar más lentamente y pueden ser más fáciles de detectar que los cambios informativos o cognitivos. Los Comandantes y sus Estados Mayores deben comprender, tanto la oportunidad de la inteligencia que reciben como los diferentes potenciales para el cambio en las dimensiones del ámbito de la

información. La implicación es que debemos tener sistemas de inteligencia y procesos organizativos ágiles para explotar este ambiente dinámico.

6. Las propiedades del ámbito de la información afectan la inteligencia: la recopilación de la información física y electrónica es medible objetivamente por la ubicación y cantidad. Si bien la identificación de grupos de interés y personas clave puede ser un desafío relativamente franco, no es fácil llegar a un acuerdo ni cuantificar sobre la importancia relativa de las diferentes personas y grupos, sus perfiles psicológicos y cómo interactúa. Los Comandantes y sus Estados Mayores deben saber apreciar la naturaleza subjetiva de los perfiles psicológicos y la naturaleza humana. También deben continuar persiguiendo los medios eficaces para intentar medir los elementos subjetivos empleando las medidas de efectividad y otras técnicas aplicables.

7. La coordinación de las Operaciones de Información planificadas con la inteligencia: debe existir coordinación entre la inteligencia, la localización de blancos, las Operaciones de Información y el personal de administración de recopilación. La necesidad de evaluaciones exactas de ganancia/ pérdida de inteligencia y políticas/ militares, al determinar los blancos a atacar y los medios a emplear es fundamental para la integración de las Operaciones de Información.

8. Análisis de las percepciones extranjeras y de los factores humanos: es necesario evaluar las percepciones extranjeras para el éxito de las actividades de las Operaciones de Información preparar el campo de batalla moderno para el éxito de las operaciones conjuntas depende de una comprensión cabal del ámbito de la información,

incluyendo las percepciones extranjeras, el análisis de los auditorios-objetivos, y el análisis cultural.
El análisis de los factores humanos, conjuntamente con la comprensión del ambiente cultural, es importante para evitar la proyección de la propensión cultural del Ecuador sobre los auditorios-objetivos. Los recursos de inteligencia contribuyen a la evaluación de las poblaciones extranjeras a través del análisis de los factores humanos, modelado de red de influencias, análisis de los medios de comunicación extranjeros, mapeo de medios, análisis de sondeo y/o grupo de enfoque, y el análisis de la influencia de los comunicadores y/o fuentes clave. Esto es, en su mayor parte, inteligencia de fuente abierta y se debe interpretar y sintetizar por expertos en la materia de inteligencia del país.

9. Requerimientos Prioritarios de Información (RPI): el requerimiento de recopilar, analizar y producir inteligencia detallada y necesaria para las Operaciones de Información actualmente excede los recursos de los organismos de inteligencia. La asignación de recursos de inteligencia a las Operaciones de Información, como sucede con todas las operaciones, se regula en base a los RPI y procesos establecidos dentro de los organismos de inteligencia. Es imperativo que se coordinen y prioricen los requerimientos de inteligencia en cada escalón de mando.

10. Las fuentes del apoyo de inteligencia: a través de la Dirección de Inteligencia del CC.FF.AA., los planificadores de Operaciones de Información tienen acceso a la inteligencia de los productores y recopiladores de inteligencia a nivel nacional y de los Comandos Operacionales. En el nivel de Comando Operacional, el Comando de Inteligencia Militar (COIM) del teatro de operaciones apoya la planificación y la ejecución de las Operaciones de

Información. Los organismos de inteligencia normalmente asignan personal específico para coordinar con los planificadores y especialistas de Operaciones de Información.

CAPÍTULO IV

RESPONSABILIDADES Y RELACIONES DE MANDO

CAPÍTULO IV

RESPONSABILIDADES Y RELACIONES DE MANDO

A. AUTORIDAD

La autoridad corresponde al poder de mandar sobre los demás, induciéndoles una determinada forma de actuar, constituye la base para la responsabilidad. Así que se trata de una relación de poder que se establece del superior hacia al subordinado, para cumplimiento de las Operaciones de Información.

La principal autoridad será el Director de Operaciones de Información, el mismo que tiene la responsabilidad de cumplir y hacer cumplir los lineamientos estratégicos y las políticas del Jefe del Comando Conjunto de las Fuerzas Armadas.

B. RESPONSABILIDADES

1. El Estado Mayor.

El Jefe de Estado Mayor Operacional tiene la responsabilidad de establecer doctrina brindando asesoramiento y hacer recomendaciones.

a) Brinda asesoramiento específico de Operaciones de Información.
b) Direcciona la planificación centralizada de las Operaciones e incluye las Operaciones de Información.

2. Director de Inteligencia (G-2)

a) Dar el apoyo y coordinar con G-6 las Operaciones de Información.

b) Proporcionar inteligencia para la selección de objetivos y análisis post ataque de las Operaciones de Información.
c) Identificar las vulnerabilidades amigas y los blancos amigos más probables dentro de las capacidades y el concepto de operaciones del adversario.
d) Desarrollar la evaluación del riesgo de inteligencia de todas las fuentes de los objetivos de las Operaciones de Información.
e) Realizar evaluaciones de los factores políticos, militares y humanos.
f) Coordinar con la Fuerza, los servicios para garantizar el apoyo de base de datos suficiente para la planificación, análisis y ejecución de las Operaciones de Información.

3. Director de Operaciones del Comando Conjunto (G-3)

a) Coordinar con las organizaciones que pudieran ser o son afectadas por la implementación de las actividades de las Operaciones de Información.
b) Integrar las Operaciones de Información en las Operaciones Militares.

4. Director de Logística del Comando Conjunto (G-4)

a) Coordinar e integrar los aspectos logísticos de Operaciones de Información en el proceso de planificación de contingencias.
b) Durante las fases de una operación deberá apoyar a los integrantes del sistema de Operaciones de Información para todas las actividades de Operaciones de Información, desde y hacia el área de responsabilidad apoyada.

5. Director de Telecomunicaciones (G-5)

a) Apoyar a las Operaciones de Información instalando, explotando y manteniendo el enlace en todos los niveles de mando.
b) Proveer estudios del área de sistemas de comunicaciones no clasificados sobre la infraestructura de sistemas de comunicaciones regionales, incluyendo las características físicas, un vistazo general de los sistemas de telecomunicaciones, y las frecuencias electromagnéticas del país y la región.
c) Proporcionar seguridad de las comunicaciones en apoyo directo a los Comandos Operacionales.
d) Facilitar informes oportunos y ajustados a los Comandantes apoyados.
e) Ejecutar en forma permanente operaciones de guerra electrónica.
f) Activar, explotar, mantener y proteger el sistema de redes informáticas del Comando Conjunto y las Fuerzas.

6. Director de Operaciones de Información (G-6)

a) Coordinar la planificación y la ejecución de Operaciones de Información entre los Comandos Operacionales.
b) Planificar y asesorar los asuntos de Operaciones de Información dentro del Estado Mayor Operacional.
c) Incluir las actividades de Operaciones de Información para apoyar el concepto de operaciones del Jefe del Comando Conjunto.
d) Recomendar las prioridades de las Operaciones de Información para lograr los objetivos planificados.
e) Recomendar a la Dirección de Operaciones (G-3), la asignación de tareas para las organizaciones, Estados Mayores y elementos que planifican y

supervisan las distintas capacidades y actividades relacionadas a utilizarse.

f) Evaluar los blancos de Operaciones de Información designados para las operaciones militares.

7. Oficial de Enlace de Guerra Electrónica.

a) Coordinar las actividades de guerra electrónica y actuar como enlace entre los departamentos de Operaciones de Información de los Comandos Operacionales y el G-6.
b) Armonizar todas las actividades de guerra electrónica y el uso militar del espectro electromagnético, dentro del área de responsabilidad del Comando Operacional.

8. Oficial de Enlace de Inteligencia.

a) Preparar inteligencia del campo de batalla de Operaciones de Información.
b) Coordinar, recopilar y evaluar, la inteligencia requerida o necesaria para las Operaciones de Información.
c) Informar sobre blancos objetivos de Operaciones de Información.
d) Evaluar riesgos de Operaciones de Información.
e) Provee pericias de seguridad física y defiende intereses e incumbencias dentro del Comando Conjunto, y el área de retaguardia conjunta según sea apropiado, durante las deliberaciones de planificación de la Dirección de Operaciones de Información.

9. Oficial de Enlace de Operaciones Psicológicas.

Analizar la información e indicativos a los auditorios objetivos a fin de planificar y ejecutar las campañas para influenciar sus emociones,

motivos, razonamiento objetivo, y finalmente el comportamiento de las organizaciones, grupos e individuos.

10. Oficial encargado de la Seguridad en las Operaciones.

a) Identifica las amenazas y vulnerabilidades existentes, desarrolla la lista de información necesaria e implementa las contramedidas de seguridad de las operaciones enemigas.
b) Monitorear la seguridad de las telecomunicaciones.
c) Coordinar con G-3 la seguridad en las operaciones militares con el monitoreo de la información que se realice.
d) En las operaciones de decepción y engaño deberá deliberadamente disuadir a los auditorios objetivos adversarios en la toma de decisiones militares sobre las capacidades, intenciones y operaciones amigas.

11. Oficial Encargado de Operaciones de Decepción y Engaño.

a) Analizar la intención del Jefe del Comando Conjunto para integrar las operaciones de decepción y engaño con la maniobra militar.
b) Planificar operaciones de decepción y engaño para integrar el Anexo de Operaciones de Información.

12. Director de Comunicación Social del Comando Conjunto.

a) Coordinar y armonizar las actividades de Relaciones Públicas, manejo de medios, producción y monitoreo de las Operaciones de Información planificadas.

b) Apoyar en las actividades que Operaciones de Información que requieren su participación.
c) Difundir las campañas de Operaciones de Información en los diferentes auditorios objetivos.
d) Disponer el monitoreo de los medios de comunicación nacional e internacional.

13. Comandos Operacionales.

a) Disponer el cumplimiento de la planificación realizada por G-6 del Comando Conjunto.
b) Planificar y ejecutar el desarrollo de las campañas de Operaciones de Información dispuestas por el G-6.
c) Evaluar la ejecución de las campañas de Operaciones de Información y reportar los resultados al G-6.
d) Participar en la planificación de las Operaciones de Información.

14. Grupos y Unidades Operacionales.

Los grupos y las unidades operacionales de cada Comando Operacional son encargados de cumplir las misiones de Operaciones de Información dispuestas por G-3.

CAPÍTULO V

PLANIFICACIÓN Y COORDINACIÓN DE OPERACIONES DE INFORMACIÓN

CAPÍTULO V

PLANIFICACIÓN Y COORDINACIÓN DE OPERACIONES DE INFORMACIÓN

A. GENERALIDADES

La planificación de las Operaciones de Información sigue los mismos principios y procesos establecidos para la planificación de las operaciones conjuntas.

El Estado Mayor, a través de las capacidades de Operaciones de Información, coordinará y sincronizará las mismas para lograr los objetivos del Comando Conjunto de las Fuerzas Armadas. Cuando las Operaciones de Información no han sido coordinadas, pueden comprometer, complicar, anular o perjudicar otras operaciones militares planificadas por el CC.FF.AA.; así como también las demás actividades de información del gobierno. El Jefe del Comando Conjunto de las Fuerzas Armadas debe garantizar que los planificadores de Operaciones de Información estén completamente integrados en el proceso de planificación y localización de objetivos, para asegurar una efectiva toma de decisiones.

B. LA PLANIFICACIÓN DE LAS OPERACIONES DE INFORMACIÓN

La planificación de las Operaciones de Información es un proceso permanente y continuo, que se emplea en todas las fases de la operación general, su empleo puede influir de manera significativa en la cantidad de esfuerzo requerido para las fases restantes.

El empleo de las Operaciones de Información en tiempo de paz para lograr los objetivos del CC.FF.AA y para impedir otros conflictos, requiere la habilidad de integrar las capacidades de las Operaciones de Información en una estrategia amplia y coherente, a través del

establecimiento de los objetivos de información que, a su vez, son integrados en los objetivos generales de la misión del CC.FF.AA y los apoyan. El plan de operaciones del Comandante operacional sirve como plataforma excelente para integrar objetivos específicos de información a largo plazo.

La planificación de las Operaciones de Información requiere una preparación temprana y detallada. Muchas capacidades de las Operaciones de Información requieren tiempo para la Preparación de Inteligencia del Campo de Batalla (P.I.C.B).

El apoyo de las Operaciones de Información para el desarrollo de la P.I.C.B es diferente a los requerimientos tradicionales y puede requerir un período de procesamiento mayor, tiene requerimientos más amplios de recopilación, producción y difusión. Por consiguiente, los Comandantes operacionales deben garantizar que se prioricen los objetivos de las Operaciones de Información de forma adecuada en sus Requerimientos Prioritarios de Inteligencia (R.P.I) y solicitudes de información.

C. CONSIDERACIONES DE PLANIFICACIÓN DE LAS OPERACIONES DE INFORMACIÓN

Es un vistazo general de las Operaciones de Información como parte de los procesos y productos de la planificación de una operación conjunta, con un enfoque en las actividades comunes del Proceso Militar en la Toma de Decisiones.

D. LA INTENCIÓN DEL COMANDANTE Y LAS OPERACIONES DE INFORMACIÓN

La intención del Comandante debe ser requerida por la Dirección de Operaciones de Información antes de que inicie la planificación específica.

Un Comandante que espere depender de las capacidades de las Operaciones de Información debe asegurarse de que se les dé una prioridad lo suficientemente alta a los R.P.I y solicitudes de información relacionados con las Operaciones de Información antes de una crisis, para que los productos de inteligencia estén listos a tiempo para apoyar las operaciones.

Como mínimo, se debe incluir la visión del Comandante para las Operaciones de Información en la guía inicial. Dadas todas las condiciones, los Comandantes proporcionan la guía sobre Operaciones de Información como parte de su concepto general, pero pueden optar por proveerla por separado. El Comandante puede elegir proporcionar una guía separada sobre las Operaciones de Información cuando sea necesario un tratamiento más focalizado y directo de las Operaciones de Información, los Comandantes pueden considerar la emisión de la guía de Operaciones de Información por separado durante los ejercicios, porque es una herramienta valiosa para adiestrar a sus Estados Mayores para ver a las Operaciones de Información como una parte esencial de su concepto general de operaciones.

E. RELACIÓN ENTRE LAS MEDIDAS DE RENDIMIENTO Y LAS MEDIDAS DE EFECTIVIDAD

1. Las medidas de rendimiento (MR) miden el cumplimiento de las tareas y las acciones de las Operaciones de Información. Las medidas de efectividad (ME) determinan si las acciones de las Operaciones de Información en marcha están teniendo el efecto deseado para el cumplimiento de la misión y la consecución de los objetivos finales.

   Las M.R miden el esfuerzo de las Operaciones de Información amigas y las M.E miden los resultados del espacio de batalla. Las M.R y las M.E de las Operaciones de Información se elaboran y

perfeccionan a lo largo de todo el proceso de planificación.

2. En el desarrollo de las M.R y/o las M.E de las Operaciones de Información, se debe tener en cuenta los siguientes criterios generales:

   a) Pertinentes

      Deben estar relacionadas directamente con los efectos deseados requeridos para lograr los objetivos.

   b) Ponderables

      La efectividad o rendimiento se miden cuantitativamente o cualitativamente. Para medir la efectividad se debe establecer una medida de base antes de la ejecución, contra la cual medir los cambios del sistema.

   c) Oportunas

      Se debe estipular de forma clara el tiempo de retroalimentación de la información requerida para cada M.R y/o M.E y elaborar un plan para presentar informes dentro de los plazos especificados.

   d) Con una asignación de recursos apropiada.

      La recopilación, el análisis y la información de los datos las M.E o las M.R requieren recursos humanos, económicos y logísticos.

      Ejemplos de M.R de las Operaciones de Información.

- Cantidad de productos de OPSIC difundidos (semanal, mensual).
- Porcentaje de instalaciones de mando y control de la amenaza que han sido afectados.
- Porcentaje de redes de computadores (A.R.C) asignadas que han sido afectadas.
- Cantidad de proyectos de operaciones cívico militares iniciados.
- El aumento de las transmisiones de la radio amenazada dentro de la frecuencia deseada, debido al ataque electrónico (A.E).
- Informes de inteligencia sobre la difusión de mensajes de OPSIC durante las operaciones militares.
- Ejemplo de M.E. de las Operaciones de Información.

M.E cuantitativas

- Porcentaje de degradación de un sistema de radar con el tiempo medido mediante un sensor apropiado.
- Cantidad y tamaño de los disturbios civiles en el tiempo según lo que han informado las fuerzas propias.
- Cantidad de intrusiones informáticas en el tiempo según han sido medidas por el software.
- Tendencias en la posición de la población objetivo sobre un asunto específico, según lo estiman las encuestas de opinión pública.
- Cantidad de tropas que se rinden según el efecto de una acción de productos comunicacionales (hojas volantes).

M.E cualitativas

- Posición del auditorio objetivo sobre un asunto específico según lo estime un grupo de enfoque o una serie de grupos de enfoque.
- Evaluación de los cambios en la sustentación (o no-sustentación) de las declaraciones públicas hechas por comunicadores clave, según se mida contra los objetivos y/o efectos de las Operaciones de Información.
- Evaluación de los cambios de tendencia de las emisoras de los medios extranjeros.
- Los casos de deserciones, rendiciones, falta de apoyo a las autoridades atribuidos al impacto y/o credibilidad de las emisiones por altavoz o las hojas volantes.

ACCIONES Y RESULTADOS DE LA UNIDAD DE OPERACIONES DE INFORMACIÓN COMO PARTE DE LA PLANIFICACIÓN CONJUNTA.		
PASOS DEL PROCESO DE PLANIFICACIÓN.	**ACCIÓN DE PLANIFICACIÓN DE LA UNIDAD DE O.I.**	**RESULTADO DE LA PLANIFICACIÓN DE LA UNIDAD DE O.I.**
Iniciación de La planificación.	Monitorear la situación. Convocar a los oficiales de O.I. Estimar el alcance inicial del papel de las O.I. Identificar los requerimientos de coordinación organizativa. Iniciar la identificación de la información necesaria para el análisis de la misión y el desarrollo de un curso de acción. Convalidar, iniciar y revisar los R.P.I y solicitudes de información. Recomendar las estrategias de las O.I y la solución de conflictos.	Solicitud de asignación de tareas para recopilar la información requerida.
Análisis de la misión.	Identificar las tareas especificadas, implícitas y esenciales de las O.I. Identificar las suposiciones, limitaciones y restricciones relevantes para las O.I. Identificar requerimientos de apoyo de planificación de las O.I. (incluyendo el aumento) y emitir solicitudes de apoyo. Iniciar el desarrollo de M.R y M.E. Analizar las capacidades de las O.I disponibles para la misión e identificar el nivel de autoridad de aprobación para el despliegue y empleo. Identificar las propiedades físicas, informativas y cognitivas relevantes del ámbito de la información. Perfeccionar los R.P.I y solicitudes de información propuestos. Proporcionar la perspectiva de O.I en el desarrollo de la misión renunciada para la aprobación del Comandante. Adaptar los pedidos de aumento a las misiones y a las tareas.	Lista de tareas de O.I. Lista de supuestos. Limitaciones y restricciones. Guía de planificación para las O.I. Pedido de aumento de las O.I. Porción de las O.I del enunciado de misión reestructurada del Comandante.
Desarrollo de un curso de acción.	Seleccionar las capacidades principales, de apoyo y relacionadas de las O.I para	Lista de objetivos de O.I para cada C.A.

	lograr tareas de O.I para cada C.A. Proporcionar los resultados del análisis de riesgo para cada C.A.	
Análisis y juego de guerra del C.A.	Analizar cada C.A. desde una perspectiva funcional de las O.I. Identificar puntos de decisión clave de las O.I. Recomendar ajustes a la organización de tareas de las O.I. Suministrar datos de las O.I para una matriz de sincronización. Identificar porciones de las O.I de operaciones derivadas y complementarias. Identificar blancos de gran valor relacionados con las O.I. Recomendar la información esencial requerida por el Comandante a las O.I.	Los datos de las O.I para la matriz de sincronización general. Porción de las O.I de las operaciones derivadas y complementarias. Lista de blancos de gran valor relacionados con las O.I.
Comparación del C.A.	Comparar cada C.A en base a la misión y las tareas de las O.I. Comparar cada C.A en relación a los requerimientos de las O.I contra los recursos disponibles de las O.I. Priorizar los C.A desde la perspectiva de las O.I.	C.A priorizados desde la perspectiva de las O.I con los pros y los contras para cada C.A.
Aprobación del C.A.	Sin ninguna acción significativa del Estado Mayor de O.I durante la aprobación del C.A.	No corresponde.
Desarrollo del plan u Orden.	Perfeccionar las tareas de las O.I del C.A aprobado. Identificar los déficits de capacidad de las O.I y recomendar soluciones. Actualizar constantemente todas las organizaciones de apoyo respecto a los detalles de la porción de las O.I de los detalles de plan (permitiendo el acceso).	Estimaciones de O.I actualizadas en base al C.A seleccionado.
Perfeccionamiento del plan	Sin ninguna acción específica del Estado Mayor de O.I durante el perfeccionamiento del plan.	No corresponde.

EJEMPLO DE LA RELACIÓN ENTRE LAS MEDIDAS DE RENDIMIENTO Y LAS MEDIDAS DE EFECTIVIDAD.			
Capacidad	**Medidas de Rendimiento (M.R)***	**Medidas de efectividad (M.E)***	**Comentarios**
Operaciones psicológicas (OPSIC).	Porcentaje de productos de OPSIC difundidos.	Grado en que las OPSIC cambiaron el comportamiento demostrado del Auditorio Objetivo.	A menudo necesita requerimientos de inteligencia adicionales.
Guerra Electrónica (G.E).	Porcentaje de instalaciones de mando y control (C2) del adversario atacadas.	Efecto de los ataques sobre la posibilidad de las instalaciones de C2 del adversario de pasar información esencial.	Las M.E requieren un cambio en una actividad detectable y medible.
Operaciones Cívico Militares.	Porcentajes de aceptación Porcentaje de actividades.	Efectos en la población propia, neutral y hostil.	Las M.E requieren un cambio en una actividad detectable y medible.
Inteligencia de O.I.	Porcentaje de información requerida y adquirida.	Inteligencia en apoyo a las O.I.	Las M.E requieren de inteligencia oportuna, completa y útil.
Seguridad en las O.I.	Porcentaje de compromisos identificados de información esencial o indicadores con medidas de operaciones de seguridad aplicadas.	Acciones del adversario observadas que demuestran la falta de conocimiento previo de las operaciones amigas.	Las M.E requieren la colación de toda la información filtrada y la comparación con las acciones del adversario.
La mayoría de las M.R se responden mediante la generación estadística interna. Las ME varían y están basadas en los objetivos de las O.I y las tareas planificadas individuales.			

CAPÍTULO V

LA EDUCACIÓN PARA OPERACIONES DE INFORMACIÓN

CAPÍTULO VI

LA EDUCACIÓN PARA OPERACIONES DE INFORMACIÓN

A. GENERALIDADES

El desarrollo de las Operaciones de Información, como un componente esencial para las operaciones conjuntas, requiere pericia y capacidades específicas en todos los niveles del Comando Conjunto. En los niveles profesionales superiores, los oficiales de grado superior desarrollan las competencias conjuntas que son la base del poder militar ecuatoriano. En cada escalón de mando, es esencial una fundamentación sólida de la educación y el adiestramiento para el desarrollo de una competencia principal. La educación y la capacitación profesional a su vez, están en función de la acumulación, la documentación y la convalidación de la experiencia adquirida en las operaciones, los ejercicios y la experimentación. Este capítulo trata la educación, el adiestramiento, el ejercicio conjunto necesario para lograr y mantener el objetivo de establecer las Operaciones de Información como competencia principal.

B. LA EDUCACIÓN EN LAS OPERACIONES DE INFORMACIÓN

Dado que la conceptualización del ámbito de la información del COMACO y el papel de las Operaciones de Información en los asuntos militares han evolucionado, se ha comprendido la necesidad de establecer los preceptos básicos de educación y adiestramiento necesarios para las Operaciones de Información de los Comandos Operacionales:

1. El personal docente de la especialidad de Operaciones de Información debe estar constituido por especialistas en las capacidades principales (Guerra Electrónica, Operaciones Psicológicas,

Operaciones de Decepción y Engaño, Seguridad en las Operaciones y Operaciones del Ciberespacio). Es necesario que los Comandantes comprendan el ámbito de las capacidades principales para asegurar la integración de las Operaciones de Información en las operaciones conjuntas.

2. El adiestramiento inicial de los especialistas en capacidades y los requerimientos de educación son específicos. Los especialistas en capacidades pueden ser oficiales o personal especialista. A medida que los especialistas adiestrados adquieren más experiencia, antigüedad y jerarquía, se debe ampliar su adiestramiento y educación para prepararlos para las responsabilidades de planificación y supervisión en el nivel estratégico militar.

3. Los planificadores de Operaciones de Información son necesarios tanto en el nivel operativo y estratégico. El personal asignado a la planificación de las Operaciones de Información en cada nivel debe tener un conocimiento práctico de las distintas capacidades que potencialmente se emplean en las Operaciones de Información; así como también de los procesos, procedimientos y herramientas de planificación apropiada, y la base legal y política para la realización de las Operaciones de Información.

4. Los miembros de las FF.AA. requieren un conocimiento de nivel ejecutivo del ámbito de la información y del papel de las Operaciones de Información y el apoyo para el logro de objetivos nacionales y/o institucionales.

C. EL ADIESTRAMIENTO DE LAS OPERACIONES DE INFORMACIÓN

El adiestramiento militar conjunto se basa en doctrina de Operaciones de Información y políticas conjuntas para el

Estado Mayor del Comando Conjunto para responder a los requerimientos estratégicos y operativos que los Comandantes consideren necesarios para cumplir las misiones que les fueran asignadas. La tarea básica de adiestramiento de las Operaciones de Información es educar al personal y a las organizaciones responsables de planificar y llevar a cabo Operaciones de Información.

El adiestramiento de las Operaciones de Información se concentra en las habilidades, metodologías y herramientas conjuntas específicas de planificación y asume un fundamento sólido de adiestramiento del Comando Conjunto, por lo que se debe tomar en cuenta lo siguiente:

1. El adiestramiento del personal militar debe dar cuenta de la naturaleza del ámbito de la información y del hecho de que las acciones individuales del personal pueden afectar las percepciones de la población. Los planificadores del entrenamiento responsables de sensibilizar a la totalidad de los participantes en el adiestramiento, sobre el impacto potencial de sus acciones individuales y colectivas sobre las percepciones de la población donde se realiza el entrenamiento, sobre todo cuando visitan lugares, donde los valores e instituciones es importante mantener su identidad y su cultura.

2. Las destrezas lingüísticas y culturales son esenciales para las Operaciones de Información. Se está aumentando la necesidad de adiestramiento cultural que son necesarias para que las unidades interactúen de manera efectiva con la población y se mantengan informadas sobre las percepciones de la población durante el desarrollo de cualquier operación conjunta.

3. Los profesionales de las Operaciones de Información necesitan la educación para ayudarlos a aprender cómo pensar en las Operaciones de Información. Las

Operaciones de Información requieren un análisis muy detallado y una habilidosa síntesis, alimentados por la pericia y los conocimientos específicos en la materia. Las Operaciones de Información exigen que los profesionales en ellas sinteticen y vean los problemas y desafíos como holísticos y relacionados en vez de verlos aislados. Por lo tanto, cada parte de las Operaciones de Información se relaciona con otras instituciones y organismos del Estado, afectan otras áreas y dimensiones geográficas.

4. La educación de las Operaciones de Información debe darle a la gente una visualización amplia de cómo afectan: las diferentes culturas del territorio ecuatoriano, la manera en que las personas piensan, planifican e interpretan los resultados. Los planificadores de Operaciones de Información también necesitan la educación suficiente para la realización de un juego de guerra que va desde la mente del Comandante amigo a las mentes de otros participantes del conflicto que ejercen influencia sobre los cursos de acción amigos.

D. LA PLANIFICACIÓN DE LAS OPERACIONES DE INFORMACIÓN PARA EJERCICIOS CONJUNTOS

El empleo eficaz de las Operaciones de Información en las operaciones conjuntas de las FF.AA. depende de la posibilidad de las mismas. Los ejercicios conjuntos proporcionan una oportunidad única de ensayar y evaluar las capacidades componentes de las Operaciones de Información. La complejidad de la integración de las Operaciones de Información en las operaciones conjuntas y el impacto que potencialmente tienen estas sobre el campo de batalla moderno, recomiendan la inclusión de las Operaciones de Información en la mayoría de los ejercicios conjuntos.

1. La planificación de ejercicios involucra todos los preparativos necesarios para estructurar el ejercicio y facilitar el adiestramiento, esto depende de G-3. La mayoría de los ejercicios conjuntos se programan en la planificación anual de ejercicios. Los resultados de esta planificación se promulgan en una directiva para los Comandos de Educación de las Fuerzas.

    a) Se puede obtener más información sobre el programa de adiestramiento conjunto en el plan anual del Comando Conjunto, tareas que deben cumplirse durante la etapa de planificación para cada ejercicio conjunto.

    b) Los aspectos de Operaciones de Información de un ejercicio deben estar relacionados con:

        1) Identificar los objetivos de los ejercicios de las Operaciones de Información que coinciden con los objetivos generales en alcance, propósito del adiestramiento.
        2) Integrar las tareas y los objetivos de las Operaciones de Información en el concepto de operaciones del jefe del Comando Conjunto para el adiestramiento.
        3) Identificar al personal con conocimientos de Operaciones de Información para participar como árbitros de control de los ejercicios conjuntos.
        4) Preparar el borrador de los departamentos de Operaciones de Información de la directiva del ejercicio y los planes de apoyo (incluyendo el plan de control del ejercicio).

2. Cuando se emplean las Operaciones de Información en los ejercicios, las consideraciones fundamentales de planificación incluyen:

a) Los objetivos del ejercicio y cómo se relacionan con las Operaciones de Información con objetivos aplicables a la realidad nacional.

b) El tipo, la ubicación y el tamaño del ejercicio, así como también la duración.

c) La representación exacta del ambiente del objetivo operacional.

d) Las lecciones aprendidas de los ejercicios y operaciones anteriores. La revisión de las lecciones aprendidas es una manera importante y rentable de evitar los errores documentados de los ejercicios y operaciones anteriores.

e) La cantidad y el tipo de las capacidades y el personal de Operaciones de Información apropiado para el tipo de ejercicios y sus objetivos.

f) El tipo de control (de juego a 1 partido (dirigido), a dos partidos (arbitrado) para las capacidades de las Operaciones de Información necesarias para lograr de forma más eficaz los objetivos de adiestramiento.

g) Definir el o las áreas “de juego” del ejercicio en el ámbito de la información. Las capacidades de las Operaciones de Información que afectan el ámbito de la información desde la actividad del ejercicio de ataque de redes de computadoras o ataque electrónico tienen el potencial para influenciar el ámbito de la información o interactuar con él fuera del área de ejercicio designada. Los planificadores de ejercicios deben evaluar el potencial para los efectos involuntarios durante todo el ejercicio. Evitar los conflictos de ejercicio con el uso del espectro de Internet o del espectro

electromagnético de terceros, involucra la adhesión a la guía provista en los procedimientos operativos normales del área de adiestramiento, así como también a los reglamentos, leyes, tratados y convenciones locales aplicables.

h) La cantidad necesaria de evaluadores experimentados de Operaciones de Información para monitorear el ejercicio de forma apropiada y ayudar en el desarrollo de lecciones aprendidas a través del proceso de informe final.

i) Para la planificación y la ejecución de los ejercicios de adiestramiento deben tener, suficiente información de inteligencia del área de empleo y la colaboración de autoridades civiles del sector, para el efectivo empleo de tácticas técnicas y procedimientos esta información debe mantener el secreto necesario.

j) Las tareas de planificación se deben emprender las siguientes tareas para garantizar que las Operaciones de Información se integren bien en los ejercicios conjuntos cuando sea apropiado.

    1) Desarrollar objetivos de ejercicios de Operaciones de Información específicos y alcanzables. La identificación y el logro de estos objetivos incrementan la capacidad para emplear los recursos de las Operaciones de Información de manera eficaz y proporcionan la herramienta para evaluar el adiestramiento del personal de las Operaciones de Información. Los objetivos deben ser medibles y compatibles con las limitaciones generales del ejercicio.

    2) El Comando Conjunto debe proporcionar oportunidades suficientes de evaluar las

habilidades de los planificadores de Operaciones de Información para coordinar las actividades de información militar, lograr los objetivos de los ejercicios, y satisfacer los requerimientos de adiestramiento. Se deben estimular las Operaciones de Información dentro de un ejercicio a través del diseño de escenarios, la participación de recursos, y la elaboración de campañas y programas de eventos específicos en el escenario donde se adiestraran las tropas.

3) Diseñar el escenario de las Operaciones de Información de manera tal que se hagan las suposiciones apropiadas sobre las capacidades de las Operaciones de Información amigas y del adversario, las percepciones básicas de las personas y grupos apropiados, así como también sobre cómo podrían cambiar durante el curso del ejercicio en reacción a las diferentes situaciones presentadas del ejercicio. Se debe proporcionar la percepción básica y la inteligencia relacionada con las Operaciones de Información en la documentación que tanto la Fuerza Azul como la Roja reciben al inicio del ejercicio. Los requerimientos técnicos y de seguridad se deben coordinar con el personal de las unidades adiestradas.

4) Obtener suficientes recursos de Operaciones de Información para apoyar los objetivos de adiestramiento durante el ejercicio. La disponibilidad de los recursos específicos puede ser difícil de programar de forma firme con meses de antelación a un ejercicio.

5) Se debe suministrar suficientes eventos relacionados a las Operaciones de

Información para mantener al personal participante motivado y conseguir los objetivos de adiestramiento.

6) Crear un ambiente de ejercicios tan realista como sea posible. El realismo se puede lograr usando las capacidades de Operaciones de Información amigas y creando modelos y simulaciones de Operaciones de Información, e incorporando modelos de respuesta de Operaciones de Información vigorosas en el ambiente de los ejercicios. Los modelos de respuesta son especialmente útiles para proporcionar la interacción con organismos en otro nivel cuando se lleva a cabo la planificación del CC.FF.AA. Con respecto a esto, debe haber una fuerza opositora bien instruida en las técnicas de información del adversario tanto en un sentido convencional como no convencional. Esta interacción también fomenta el juego de guerra de Operaciones de Información para la superioridad de información.

7) Garantizar la asignación de personal adecuado para las funciones y las evaluaciones del adiestramiento de Operaciones de Información.

8) Considerar el garantizar operaciones de seguridad “del mundo real” en la planificación del ejercicio. Coordinar con las autoridades apropiadas para garantizar que se aplique la protección de la información de los ejercicios para evitar la fuga de información que puede ser útil para el adversario.

k) El flujo de la planificación de ejercicios de las Operaciones de Información y sus tareas de

planificación tratadas en el párrafo anterior se deben cumplir dentro del marco de las fases de la planificación de ejercicios que culminan en el informe y las lecciones aprendidas.

3. Preparación, ejecución y evaluación posterior al ejercicio de las Operaciones de Información:

   El escenario de planificación es solamente la primera de las cuatro etapas del ciclo de cada ejercicio conjunto. Las otras tres etapas: la preparación, la ejecución y la evaluación posterior al ejercicio, también involucran las tareas y la coordinación de parte del personal de Estado Mayor del ejercicio de las Operaciones de Información.

   a) Escenario de Preparación

   Durante la etapa de preparación, se distribuye la directiva y los planes de apoyo aprobados del ejercicio se desarrolla y lleva a cabo el adiestramiento previo al ejercicio; se finalizan y se prueban todas las bases de datos específicas del ejercicio; y se convalidan las tácticas técnicas y procedimientos del ejercicio. Durante esta etapa se asigna recursos y se aprueba el plan. Los preparativos de las Operaciones de Información durante este período incluyen obtener las autorizaciones y notificaciones necesarias para la actividad de las Operaciones de Información coordinar la implementación de la directiva del ejercicio, y dar lugar a los cambios del personal y los recursos.

   b) Etapa de Ejecución

   Durante la realización del ejercicio, el personal responsable de las Operaciones de Información debe concentrarse en garantizar que los eventos

de las Operaciones de Información estén planificados y orientados y éstos ocurran como ha sido planificado, que las actividades del ejercicio de las Operaciones de Información reales se mantengan concentradas en los objetivos de adiestramiento y que los datos y las observaciones que apoyan el proceso del Informe final se recopilen y procesen de forma apropiada.

c) Etapa de Evaluación Posterior al Ejercicio

Este período comienza en realidad antes de la conclusión del ejercicio. Las actividades de las Operaciones de Información asociada con esta etapa incluyen la convalidación y documentación de las lecciones aprendidas, la participación en las reuniones y la coordinación del retorno de los participantes y recursos a los repartos a los que pertenecen.

E. LAS OPERACIONES DE INFORMACIÓN EN EL ENTRENAMIENTO CONJUNTO

La conceptualización del ámbito de la información y de la actividad militar dentro de él continúa en evolución. El proceso de experimentación conjunta provee los medios para realizar el análisis estructurado de los conceptos de operaciones, la doctrina, y las capacidades específicas de las Operaciones de Información en un ambiente controlado. Este proceso es crucial para establecer, medir y convalidar las tácticas; las técnicas, los procedimientos y las capacidades propuestas de las Operaciones de Información para asignar los recursos de manera eficiente.

El adiestramiento del personal provee al personal de Operaciones de Información las habilidades para el empleo de las capacidades y lograr que el mando superior

y el ambiente civil involucrado entiendan la evolución de los nuevos escenarios de la guerra moderna.

Las recomendaciones que resultan de los ejercicios de las Operaciones de Información se mantengan y se asignen los recursos para las tropas de Operaciones de Información y unidades de empleo de las FF.AA., con ello se logra que se adiestren y se mantengan operativamente acorde.

APÉNDICE A

INSTRUCIONES ADMINISTRATIVAS

1. Comentarios de Usuarios.

Se solicita encarecidamente a los usuarios de este manual que en el campo que presenten comentarios sobre esta publicación esta publicación dirigirlo a los señores: Jefe del Comando Conjunto de las Fuerzas Armadas, Director de Educación y Doctrina Militar del CC.FF.AA., Director de Operaciones de Información.

2. Autoría.

El patrocinador de la doctrina en el Comando Conjunto de las Fuerzas Armadas es el: Director de Educación y Doctrina Militar del CC.FF.AA. (DIEDMIL).

3. Recomendaciones de cambio.

a) Las recomendaciones de cambios urgentes a esta publicación se deben presentar:

1) Dirección de Doctrina del CC.FF.AA. (DIEMIL)
2) Dirección de Operaciones de Información (G-6)

Los cambios rutinarios se deben presentar al Director de Educación y Doctrina del CC.FF.AA y al Director de Operaciones de Información del CC.FF.AA.

b) Cuando una Fuerza, Dirección, Escuela o Instituto presente una propuesta al manual de Operaciones de Información:

Donde cambie la información de los documentos originales reflejadas en esta publicación, dicha entidad incluirá un anexo a su propuesta.

c) Registro de los cambios:

NUMERO DE CAMBIO	NÚMERO DE COPIA	FECHA DEL CAMBIO	FECHA DE INGRESADO	ENVIADO POR	COMENTARIOS