RESERVADO **ME 11-13**

EJERCITO DEL PERÚ

COMUNICACIONES

OPERACIONES DE

INFORMACION

JUL – 2,004

COMUNICACIONES

OPERACIONES DE INFORMACION

INDICE

ANEXOS:

CAPITULO 1
INTRODUCCION

SECCIÓN I. GENERALIDADES

01. FINALIDAD

a. Este manual direcciona el contexto operacional de las **OPERACIONES DE INFORMACION (OI)**, la nueva terminología relevante a dichas operaciones y el medio ambiente de las mismas. Ha sido formulado para servir de guía a los G-6's (S-6's), los Cmdtes de Unidades de Comunicaciones y de Guerra Electrónica, y en general para los comandos y sus estados mayores que conduzcan o participen en las operaciones de información, relativas al comando y control de sus fuerzas.

b. El contenido de este manual también puede servir para apoyar al proceso de planeamiento de las operaciones conjuntas y durante la ejecución de las misma, en cuanto se relacionen a las operaciones de informaciones; en los niveles operacional y táctico.

02. ALCANCE

a. Este manual puede emplearse para todo el rango de las operaciones militares sea que éstas se realicen en tiempo de paz, en conflicto o en guerra, ampliando considerablemente la doctrina desarrollada para las Comunicaciones, para la Guerra Electrónica (GE) y para el comando y control (C^2) de las fuerzas, elementos tradicionales relacionados con la información.

b. El foco u orientación está sobre un nuevo concepto denominado **GUERRA DE COMANDO Y CONTROL (G-C^2)**, aunque también abarca aspectos relacionados a asuntos civiles y a relaciones públicas; y otras materias que permitirán al Ejército y a las organizaciones conjuntas "Ganar y mantener el dominio de la información, así como un efectivo C^2"

c. La doctrina desarrollada en este manual ayudará a los líderes, a los estados mayores (EEMM) y a la tropa en general que ejecuten o conduzcan OI en apoyo a las operaciones militares; así como les servirá de fundamento para desarrollar nuevas tácticas, técnicas y procedimientos (TTP); refinar o mejora: las currículas o estructuras curriculares de las escuelas de formación, perfeccionamiento, capacitación y/o especialización; y, los ejercicios de unidad, gran unidad y conjuntos.

03. CONSIDERACIONES INTRODUCTORIAS

a. El Ejército va iniciar un proceso de modernización de todos los estamentos de su estructura organizativa, en un momento en que el mundo esta caracterizado por un acelerado crecimiento del volumen de la información, de las fuentes de información y de las posibilidades de difundir información; apoyado por la tecnología de la información. Este momento es conocido como **"La era de la información"**, la que ofrecerá oportunidades únicas, pero también formidables retos. La introducción de nueva tecnología en el Ejército mejorará su habilidad para el dominio situacional sobre el terreno o territorio, elemento decisivo de la victoria, que siempre ha sido crítico; ya que el potencial adversario también empleará muchas de estas mismas

tecnologías modernas; produciéndose una lucha o guerra por tener el dominio de la información, cuyo vencedor tendrá un efectivo C^2. Un efectivo C^2, es una necesidad para las operaciones exitosas, pues transformarán las posibilidades militares en poder militar aplicado. Cuanto más efectivo es el sistema de C^2 de una fuerza, más completas serán sus posibilidades de realización en paz o en guerra.

b. En respuesta a los retos y oportunidades de la era de la información, el Ejército deberá preparar a sus combatientes para participar en operaciones de paz o en guerra para el siglo XXI. La información y el conocimiento están fluyendo en todas direcciones, las tropas y sus líderes deben ser capaces de transformarlas en posibilidades donde estén integrados todos los aspectos de información para cumplir o alcanzar la potencialidad total que mejore la conducción de operaciones militares.

c. Las operaciones de información (OI) no son nuevas; en su forma más simple ellas son las actividades que se realizan para obtener información y conocimiento que mejoren la ejecución de las operaciones amigas, al mismo tiempo que se niega al enemigo posibilidades similares por cualquier medio posible. Los efectos de las OI producen ventajas militares significativas para las fuerzas que conducen tales operaciones.

d. La información es un fundamento esencial de la guerra basada en el conocimiento, posibilitando a los Comandantes coordinar, integrar y sincronizar las funciones de combate sobre el campo de batalla. Para ganar la relativa ventaja de posición (maniobra) y concentrar los efectos (poder de fuegos), los Cmdtes deben actuar cuando la información sea relevante y antes que el adversario pueda reaccionar. El objetivo o blanco de las IO debe ser el ataque al flujo de información del adversario o más propiamente dicho a sus sistemas de información, a la vez que protegemos los nuestros; lo que contribuirá directamente a las operaciones decisivas, al poder influir en la percepción de la situación o al prevenir la tenencia o empleo de información relevante por parte del adversario.

e. El dominio absoluto y sostenido del ambiente de la información no es posible; de ahí que los Cmdtes buscarán alcanzar el dominio de la información sólo en el lugar, momento y circunstancias correctas, definiendo como ve el adversario el campo de batalla aeroterrestre y creando la oportunidad para lograr la iniciativa y sentar el ritmo de las operaciones:

   (1) La precisión, la letalidad y el alcance de las armas modernas han forzado a los Cmdtes a dispersar sus formaciones, así como a descentralizar el control y ejecución. Concentrar los efectos de estos sistemas dispersos dependerá de información precisa, igualmente la dislocación del flujo de información o la degradación de la misma, puede negar los efectos de las armas y sistemas. En lugar de verse limitado a la destrucción física de las tropas y de las máquinas de guerra como el único medio para tener éxito en el campo de batalla, hoy en día los ejércitos modernos pueden atacar y buscar anular los sistemas de información del adversario, alterando la "química" del campo de batalla y haciendo que el éxito sobre él sea prácticamente un hecho en poco tiempo.

   (2) La velocidad y la penetrante dominación de la transmisión de datos en la era de la información, están causando un cambio revolucionario en la naturaleza de las operaciones militares y en la propia guerra. La información como blanco u objetivo se extiende más allá del campo de batalla, envolviendo más que un ataque al flujo de información

adversario mientras protegemos el flujo de información amigo; requiere que estemos conscientes y sensitivos a la info publicada por fuentes no-militares, las cuales son capaces de proporcionar info de nivel táctico en tiempo casi real para audiencias globales no sólo en territorio nacional o dentro de un teatro de guerra, sino alrededor del mundo, con la potencialidad de influenciar profundamente el contexto de estas operaciones militares.

(3) Las OI definen la situación operacional mediante la generación de su entendimiento, proporcionando el contexto e influenciando las percepciones. Ellas son capaces de proteger los **Sistemas de información (SINFOR)** amigo; sincronizar la aplicación de la fuerza; conectar sistemas jerárquicos y no-jerárquicos; enlazar sensores, base de fuegos y Cmdtes; y degradar, dislocar o explotar las operaciones adversarias atacando su C^2. Todas las unidades del Ejército, debidamente entrenadas en la doctrina que se desarrolla en este manual, podrán conducir OI a través de todo el rango de la operaciones militares; permitiendo a sus comandantes expandir sus espacio de batalla (Ver ME 11-30 Ed 1999), incluyendo la interacción con los medios, la industria o proveedores, otros institutos armados, dependencias públicas o privadas relacionadas con la defensa nacional y hasta con redes globales de computadoras.

f. A pesar de la posible sinergia del poder de la información con la tecnología de la información, aún podría quedar algún velo o fricción por resolver además del reto de ordenar las Telemática desde en medio del ruido de una masa de datos expandiéndose. Muchas soluciones al dilema de incertidumbres para el Cmdte serán técnicas, pero ellas no podrán visualizarse sin la influencia humana y la comprensión de él y de sus subordinados, quienes enlazan e integran información, tecnología y acción. Las operaciones de información no ofrecen ninguna panacea, pues el conocimiento perfecto no es su objetivo, por lo tanto el objetivo militar sigue vigente: entrar a un teatro operacional con la capacidad de alcanzar una superior potencia combativa relativa contra un enemigo o establecer un dominio situacional en otras operaciones de no-guerra.

g. El manual de operaciones (ME 100-5) describe como piensa el Ejército acerca de la conducción de operaciones y el manual de organización y operaciones de EM (ME 11-30 Ed 1999) como planear, controlar y supervisar las mismas. Este manual busca acomodar y balancear las nuevas tecnologías de información emergentes, especialmente las digitalizadas, explicando los fundamentos de las operaciones de información para el ejército y orientándose hacia una estrategia militar conjunta de guerra de comando y control ($G\text{-}C^2$) que debe implementarse, buscando:

(1) Identificar información que influencia de manera importante sobre las operaciones en los niveles tácticos, operacional y estratégico.

(2) Posibilitar que los Cmdtes tengan éxito en integrar información, SINFOR y sus efectos a través de todo el rango de operaciones militares, que contribuya y mejore los elementos de la potencia combativa.

(3) Crear sinergia, que contribuya a incrementar la letalidad, supervivencia y el ritmo en el combate.

SECCIÓN II. AMBIENTES TECNOLOGICOS Y GEOESTRATEGICOS DE LA INFORMACION

04. OPERANDO EN LA ERA DE LA INFORMACION

a. Los Cmdtes y sus EEMM que operan en la era de la información enfrentan un ambiente complejo creciente; ellos en todos los niveles encontrarán un campo de información en expansión denominado **"Ambiente de Información Global (AIG)"**; que contiene aquellos sistemas y procesos de información que están más allá de la influencia directa de las autoridades militares y tal vez aún de las nacionales, pero que sin embargo pueden impactar directamente sobre el éxito o fracaso de las operaciones militares. Los medios de comunicación, los sistemas de telecomunicaciones públicos y privados, las organizaciones internacionales y aún los individuos con o sin cierto poder, representan una lista parcial de los protagonistas del AIG.

b. Los párrafos y secciones subsiguientes describen el campo o espera de influencias del AIG e introducen el concepto de "Dominio de la Información", como un elemento clave para operar con efectividad dentro de este nuevo ambiente. Para alcanzar el dominio de la información, el Cmdte debe ser hábil en el manejo de la tradicional maniobra orientada en el campo de batalla y en el "Ambiente de información militar (AIM)", definida como aquella porción del AIG relevante a su operación. Para lograr lo último (dominio del AIM), el Cmdte dirige la obtención, el empleo y la administración de la información amiga y enemiga, así como conduce las operaciones de la G-C^2.

05. EL AMBIENTE GEOESTRATEGICO - TECNOLOGICO

a. Debido al rápido avance en la tecnología, especialmente en el campo de la información, el ambiente geoestratégico de hoy ha llegado a ser tremendamente complejo y lo será aún más en el futuro. Las comunicaciones globales han acelerado y expandido la conciencia colectiva de los eventos, asuntos e intereses; despertando pasiones, desencadenando nuevas perspectivas, cristalizando profundos pensamientos o creencias ideológicas; y obligando a la gente, organizaciones, instituciones y hasta naciones de todas partes del mundo a examinar, definir y actuar sobre sus propios intereses. A pesar que muchos efectos de este fenómeno pueden ser benignos y beneficiosos, otros crearán turbulencias, confusión, caos y conflictos; estos últimos pueden extenderse más allá de un campo de batalla tradicional para comprender actividades tales como el espionaje, sabotaje, terrorismo, competencia económica y esfuerzos por captar percepciones públicas favorables.

b. En la era de la información, nuestro país es dependiente de la moderna tecnología proveniente de países desarrollados y de grandes corporaciones multinacionales que dominan y controlan los sistemas de telecomunicaciones y los flujos de difusión y/o concentración de información. Nuestras estructuras civiles, sociales y económicas, así como los gobiernos locales, provinciales, departamentales y regionales, están llegando a ser dependiente de la rapidez y precisión de ese flujo, que esta cimentado sobre una "Infraestructura de Información Global (IIG)" que enlaza electrónicamente organizaciones e individuos alrededor del mundo y que está caracterizado por emergentes tecnologías y redes de información tanto para uso civil como militar.

c. El desarrollo de la tecnología de la información revolucionará y de hecho ya ha cambiado la forma como las naciones, organizaciones y la gente interactúan. La rápida difusión de la información, posibilitada por los avances tecnológicos, reta la relevancia de los principios tradicionales de organización y administración. Para los militares, las implicancias de la nueva ciencia organizacional que examina interedes y modelos de administración jerárquicos versus no-jerárquicos, no está aún ni meridianamente entendida, sin embargo, puede predecirse que la tecnología de la era de la información y la administración de ideas, promoverán o provocarán una gran influencia sobre las fuerzas armadas, las organizaciones militares, el equipamiento y la manera como entrenar, como combatir y como protegerse durante la solución de un conflicto o guerra.

06. EL AMBIENTE DE INFORMACION GLOBAL (AIG)

a. El AIG incluye todos los individuos, organizaciones o sistemas, muchos de los cuales están fuera del control de autoridades civiles o militares nacionales; que reúnen, procesan y difunden información a las audiencias nacionales e internacionales. Todas las operaciones militares se llevarán a cabo dentro de ese AIG, que es tanto interactivo como penetrante en su presencia e influencia.

b. La actual y emergente tecnología electrónica permite que cualquier aspecto de una operación militar pueda ser conocido por una audiencia global en tiempo casi real y sin el beneficio de filtros o censuras. Con el fácil acceso a redes de información global o nacional; la supresión, el control, la censura o las limitaciones de la difusión de informaciones puede no ser posible ni tampoco deseable en muchas circunstancias.

c. Los potenciales adversarios y hasta organizaciones hostiles emplearán el AIG para introducirse en el ambiente de información militar (AIM), para lo cual emplearán sistemas y organizaciones internacionales globales con capacidad para navegar por las "Supercarreteras de la información", buscando afectar la dirección estratégica y operacional de las operaciones militares, aún antes que ellas empiecen. Independientemente del control militar, su impacto será siempre dependiente de la situación, pudiendo causar un efecto no-anticipado o no-intencional sobre dichas operaciones militares. Los protagonistas de dichos sistemas u organizaciones pueden ser:
   (1) Dependencias del gobierno.
   (2) Organizaciones no-gubernamentales (ONG's)
   (3) Organizaciones privadas de voluntarios (OPV's)
   (4) Agencias internacionales que proporcionan un servicio comercial tales como la agencia espacial europea para lanzar satélites).
   (5) Agencias que coordinan los esfuerzos internacionales, tales como el comité internacional de la Cruz Roja o la organización mundial de la salud.
   (6) Elementos sociales y culturales, incluyendo movimientos religiosos y sus líderes.
   (7) Sistemas de Comunicaciones militares e inteligencia de otras institutos y de los adversarios.
   (8) Individuos con Hardware y Software apropiados para comunicarse con audiencias globales.

d. Conforme la tecnología posibilita que un mayor número de individuos, grupos, organizaciones y naciones, puedan establecer enlace con el

mundo a través del AIG, los protagonistas de los sistemas podrían suponer que ellos persiguen sus intereses; por lo que buscarán protegerlos mediante la manipulación y control del contenido y del flujo de información dentro del AIM. Ver figura 1.

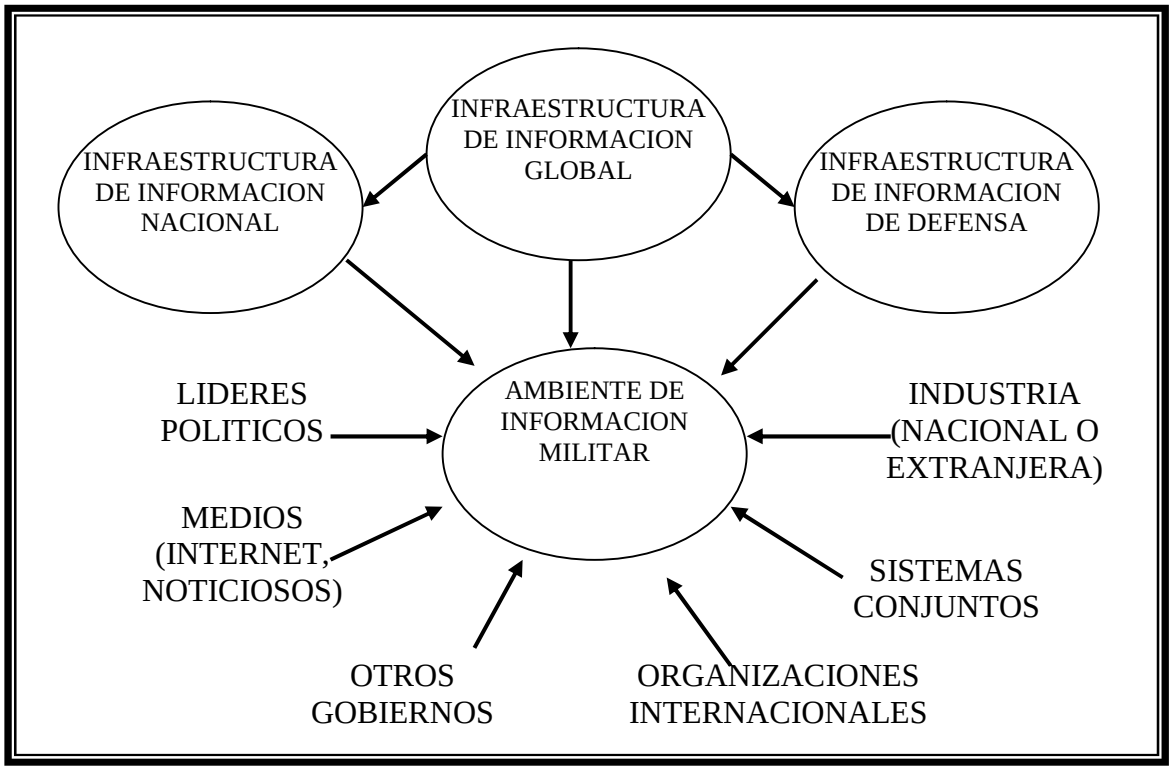

FIGURA 1: AMBIENTE DE INFORMACION GLOBAL

07. LOS MEDIOS NOTICIOSOS

a. El rol de los medios noticiosos continuará expandiéndose. El número de organizaciones de noticias y sus medios para obtener, procesar y difundir información esta incrementándose exponencialmente. Ellos buscarán por cualquier vía estar presente, mediante sus reporteros, dentro de cualquier operación militar para cubrirla. Probablemente la demanda del público nacional e internacional para conocer que esta pasando, empujará y alentará a los medios a intentar participar activamente en la operaciones militares.

b. El manual de operaciones (ME 100-3 Ed 1997) en su párrafo 11, reconoce que el impacto de la cobertura de los medios (prensa), puede afectar dramáticamente la dirección estratégica y el rango de las operaciones militares; al ser un factor influyente en los criterios operativos. Claramente, el efecto de lo escrito y más importante, la información visual proyectada por organizaciones noticiosas, directa y rápidamente; influirán la naturaleza de las políticas, objetivos y empleo de las fuerzas militares en los conflictos y guerras.

08. EL AMBIENTE DE INFORMACION MILITAR (AIM)

a. El AIM está definido como aquel que este contenido dentro del AIG y que incluye SINFOR y organizaciones (amigas y enemigas, militares y no-militares) que apoyan, posibilitan o influencian significativamente una operación militar específica. Este AIM debe considerar como mínimo:
   (1) El empleo de plataformas satelitales desde y hacia la zona de operaciones.
   (2) Un tiempo adecuado, desde una fase de alerta hasta otra de redespliegue.
   (3) Un propósito por alcanzar, desde una misión táctica hasta un estado final económico y social, político y/o diplomático.
   (4) Incluir a la gente, desde los soldados desplegados o movilizados, sus familias, la población local o regional, hasta una audiencia global; todos los cuales pueden ser impactados por la información.

b. Dentro del contexto de un AIM, los líderes del Ejército que ejercitan el comando de batalla enfrentarán muchos nuevos retos y también tendrán muchas nuevas oportunidades operacionales; y para realizarlas necesitarán que las OI lleguen a ser una parte integral de la dimensión total de las operaciones.

c. Las relaciones entrelazadas entre los factores estratégicos - geopolíticos, la tecnología y la administración de recursos; requerirán la adopción de una nueva perspectiva. La proliferación de SINFOR y la explosión de la información global traerá más protagonistas en el espacio de batalla; implicará nuevas formas de administrar las fuerzas; comprimirá los tradicionales niveles de la guerra en tiempo y en espacio; y dará a las operaciones un carácter simultáneo y continuo. Un espacio de batalla de un Cmdte incluye ahora conectividad de información global; por lo tanto las acciones militares tácticas pueden tener implicaciones políticas y sociales, que él debe considerar cuando planee, se prepare y conduzca operaciones.

d. Conocer la situación actual requerirá un enfoque y preocupación adicional en factores no militares. Los Comandantes pueden balancear mejor los efectos de la nueva tecnología sobre sus organizaciones, mediante el empleo de nuevo y emergente planeamiento automatizado y ayudas de decisión, así como con el empleo de nuevos o diferentes métodos y técnicas de control y administración.

SECCIÓN III. INFRAESTRUCTURAS DE INFORMACION

09. COMPONENTES DE LA INFRAESTRUCTURA DE INFORMACION

a. Dentro del AIG, un intricado grupo de infraestructuras de información han envuelto a los enlaces individuales, de grupos y de naciones en una red comprensiva; que distribuye el creciente y veloz flujo de información a todos los elementos que tengan acceso a la red. En la práctica, subelementos etiquetados están induciendo a interpretar que el ambiente de información no tiene límites discretos. Cada subelemento esta inextricablemente entrelazado, una tendencia que se intensificará con la continua aplicación del rápido avance tecnológico.

b. Esta red comprensiva lo constituye un enmarañado de telecomunicaciones mundiales (Worldwide web) que trasciende la industria, los medios y a los

militares; e incluye entidades de gobierno y no gubernamentales enmarcadas en:

(1) La infraestructura de información global (IIG)
(2) La infraestructura de información nacional (IIN)
(3) La infraestructura de información de defensa (IID)

c. Infraestructura de Información Global (IIG)

(1) La IIG es una interconexión de redes de telecomunicaciones, computadoras, bases de datos y consumidores electrónicos, que colocan una vasta cantidad de información en las yemas de los usuarios. La IIG es un término que abarca todos estos componentes y captura la visión de un amplio, perfecto y dinámico mecanismo de redes de trasmisión; aparatos de información, contenidos y gente.

(2) La accesibilidad global y el empleo de información en la IIG es especialmente crítico, dada la creciente globalización de los mercados, recursos y economías; considerando que:

(a) Incluye más que sólo facilidades físicas empleadas para almacenar, procesar y materializar voz, datos e imagen; engloba un amplio arreglo de posibilidades sobreexpandidas que incluyen cámaras, escaneadores, teclados, facsímil y otras máquinas periféricas.

(b) Electrónicamente enlaza organizaciones e individuos alrededor del globo y que está caracterizado por emergente redes y tecnologías de información civiles y militares.

d. Infraestructura de Información nacional (IIN)

(1) Todas las IIN's son una parte integral de la IIG y sus componentes la reflejan pero a escala reducida.

(2) La IIN es:

(a) Una serie de componentes, incluyendo la reunión de redes públicas y privadas de alta velocidad, interactivas, interconectadas y de banda angosta y banda ancha.

(b) Un conjunto de tecnologías de comunicaciones satelitales, terrestres e inhalámbricas que entregan informaciones a hogares, negocios y otras instituciones públicas y privadas.

(c) Información y contenido que fluye sobre la infraestructura sea en forma de base de datos, palabra escrita, imagen televisiva, voz o software de computador.

(d) Computadoras, televisores y otros productos que emplea la gente para accesar a la infraestructura.

(e) La gente quién provee, administra y genera nueva información y aquella que ayuda a otros a hacer lo mismo.

e. Infraestructura de Información de Defensa (IID)

Es aquella que comprende la transferencia de información y los recursos de procesamiento, incluyendo almacenamiento de información y datos, su manipulación, su recuperación y su exposición. La IID interconecta la red de comando y control, computadoras de apoyo a la inteligencia y a los usuarios mediante servicios de voz, datos, imagen, vídeo y multimedia;

proporcionando procesamiento de información y servicios de valor agregado a suscriptores militares de la Red del Sistema de Información.

10. AMENAZAS A LA INFRAESTRUCTURA DE INFORMACION

a. Las amenazas a la infraestructura de información son genuinas, globales en origen, técnicamente multifacéticas y en crecimiento; que pueden prevenir de individuos y/o grupos motivados por razones militares, políticas, sociales, culturales, étnicas, religiosas, personales, económicas e industriales; que perturban, alteran, hurtan, manipulan o destruyen los sistemas de información (SINFOR); sea para amenazar o simplemente para demostrar su habilidad.

b. La globalización de las redes de comunicaciones han creado vulnerabilidades debido al creciente acceso a la infraestructura de información desde diferentes puntos alrededor del mundo. Las amenazas contra las computadoras, sistemas de computadoras y redes varían por el nivel de hostilidad (paz, conflicto o guerra), por las posibilidades técnicas y por la motivación. Ver figura 2.

c. Como se aprecia en la figura 2 en el plano inferior, en el lado derecho se mencionan las principales amenazas o adversarios de los niveles estratégicos hasta tácticos los cuales pueden estar estructurados (militares) o no-estructurados (usuarios no autorizados), conformando una variedad de nuevas y diferentes fuentes y que existen sobre una continuidad básica aún durante períodos de paz relativa. En el mismo plano en la parte inferior se muestran algunas opciones del adversario que podrían usar para influir o atacar a los SINFOR y servicios del oponente; tal atq' puede ser diseñado con un efecto de retardo tal como la corrupción o degradación de una base de datos o el control de un programa; o también como una acción inmediata como el atq' electrónico o la destrucción física con armas convencionales. Ejemplos de estas opciones incluyen:

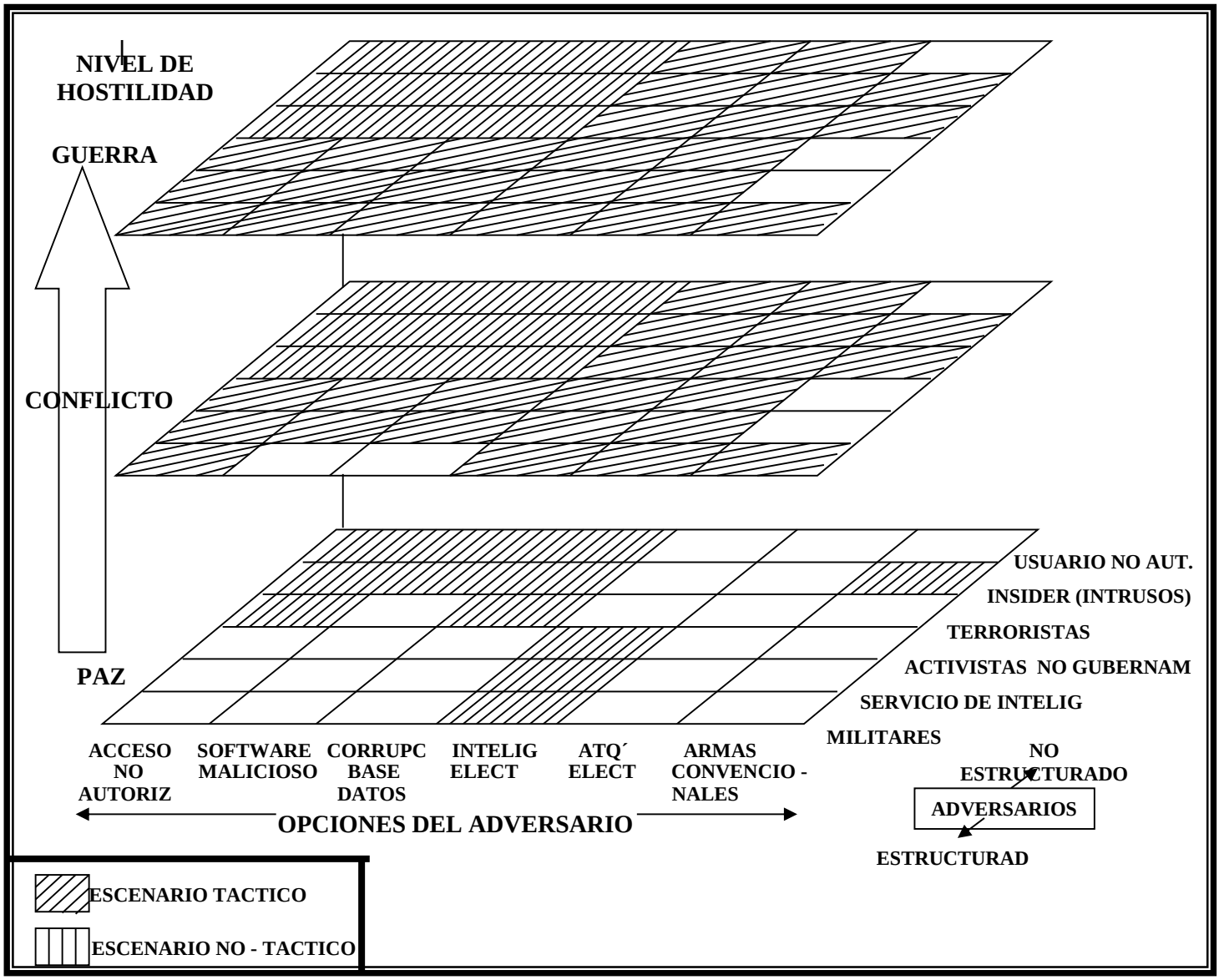

FIGURA 2: AMENAZAS A SISTEMAS DE INFORMACION

(1) Acceso no autorizado, tanto para obtener información o insertar datos.
(2) Insertar Softwares maliciosos para causar que un computador opere de manera diferente a la intentada por su usuario autorizado. Esto incluye virus informático de computador, bombas lógicas y programas diseñados para sobrepasar programas de protección.
(3) Corrupción de base de datos a través del empleo de software malicioso, alteración de datos o el empleo de ataque electrónico para hacer que se pierda, lleve a error, se malinterprete o sea inutilizable dicha base de datos.
(4) Reunión de inteligencia electrónica, sean Telemática, radiación o datos.
(5) Conducción de acciones de ataque electrónico tales como perturbación, difusión de Telemática falsas o generación de ráfagas de pulso electromagnético.
(6) Empleo de operaciones sicológicas y engaño para influir sobre los SINFOR amigos.
(7) Ataque para la destrucción física, degradación o dislocación o desorganización de comunicaciones militares y redes de control o

sistemas civiles con los cuales se interconectan las operaciones militares. Las armas empleadas para tales esfuerzos van desde bombas terroristas, artillería, fuerzas especiales hasta helicópteros y aviación.

(8) Empleo de la perturbación y trasmisiones de engaño para atacar los sistemas de comunicaciones comerciales sobre los cuales el ejército pasa alguna información.

d. La efectividad de las operaciones militares puede degradase si la confianza del usuario en la calidad de los datos puede erosionarse. Datos espurios o Telemática falsas podrían trasmitirse para erosionar la confianza en la precisión y efectividad de tales sistemas críticos, como por ejemplo sobre los sistemas de posicionamiento global o GPS.

e. Fuentes de amenaza o adversarios:

(1) Como se ha manifestado las amenazas provienen de una serie de fuentes, desde los individuos (usuarios no autorizados o insiders o infiltrados) hasta organizaciones nacionales complejas (servicios de inteligencia extranjeros y militares adversarios). Los límites o fronteras entre estos grupos son indistinguibles y a menudo es difícil discernir el origen de cualquier incidente particular. A continuación se describe brevemente cada una de las seis principales fuentes mencionadas en la figura 2.

(2) Usuarios no autorizados, tales como los piratas, son la fuente que más ataca a los SINFOR en tiempo de paz. Aunque a la fecha, ellos han atacado principalmente a computadores personales; la amenaza que tienen a las redes y computadores tipo mainframe es creciente.

(3) Insiders (infiltrados), son los individuos con acceso legítimo a un sistema o información confidencial. Cuando dichos individuos son reclutados o automotivados por cualquier organización o razón contraria a la organización a que pertenece, se convierten en la amenaza más difícil de la cual defenderse, ya que precisamente ellos conocen cual es la forma de protegerse contra ese ataque. Aunque un insider (infiltrado) pueda atacar un sistema en casi cualquier momento durante su período de vida (del sistema), los períodos de mayor vulnerabilidad para un sistema son durante su diseño, su producción, su transporte y su mantenimiento.

(4) Terroristas, son aquellos cuyas acciones van desde el acceso no autorizado a una red de información hasta el ataque directo contra la infraestructura (con bombas). Se han identificado también grupos terroristas que usando computadoras anuncian pasar inteligencia y datos y técnicos a través de fronteras internacionales.

(5) Grupos o activistas no gubernamentales, son los nuevas actores, que van desde los carteles de drogas hasta activistas sociales, que toman ventaja de las posibilidades ofrecidas por la era de la información. Ellos pueden adquirir, a bajo costo, las posibilidades para golpear las infraestructuras de comunicaciones y de seguridad de sus enemigos comerciales, políticos, sociales, policiales, etc. Mas aún, ellos puedan atacar con relativa impunidad desde distancias alejadas a sus objetivos, así como emplear los medios de comunicación internacional para intentar influir en la opinión pública global y formar percepciones de un conflicto; o pueden inflamar asuntos o temas dormidos, latentes u olvidados para que se conviertan en conflictos, que de otra manera no surgirían.

(6) Servicios de Inteligencia foráneos, que están activos durante los periodos de paz y conflicto, tomando ventaja de la oferta anónima por computador para ocultar su organización de búsqueda y reunión o para desorganizar actividades del oponente protegidos por la fachada de piratas no organizados. Sus principales objetivos son a menudo redes científicas o comerciales más que ataques directos sobre lo militar.

(7) Militares o políticos opuestos.- Aunque las actividades de estas fuentes están tradicionalmente más asociados con conflictos abiertos o guerra, su manipulación de medios de comunicación durante tiempo de paz pueden ayudarlos a enmarcar la situación a sus intereses o para su ventaja antes que se inicien las hostilidades.

f. Niveles de hostilidad

(1) El nivel de hostilidad generalmente refleja el propósito y escala de las acciones adversarias contra los SINFOR amigos. En tiempo de paz, el acceso no autorizado y uso de computadores, sistemas de computación y redes; son actualmente las más grandes amenazas. El empleo deliberado de software malicioso por un adversario podría usarse contra sistemas de comunicaciones, transportes, bancos, energía y computación; de los cuales depende o podrían depender tanto la industria, el comercio y hasta los militares. Se debe esperar que un adversario use software malicioso para evaluar la vulnerabilidad de nuestras redes de información.

(2) Conforme una crisis se vaya desplazando hacia derivar en un conflicto o guerra, pueden surgir ataques más directos y de mayor alcance contra la información y SINFOR. Los objetivos pueden incluir tanto unidades como sus infraestructuras de apoyo. Durante el despliegue de unidades tácticas se podrían ver los resultados de las primeras intromisiones e inserciones, permitiendo que el software malicioso insertado o introducido paralice los sistemas o degrade las comunicaciones. Cuando la unidad se encuentre enganchada en combate, podría haber sido objeto de una variedad de ataques cubiertos o encubiertos contra sus SINFOR.

(3) En el campo de batalla, la dependencia en una infraestructura de comunicaciones extensa y potencialmente frágil presenta una vulnerabilidad que atrae a su explotación. Los candidatos iniciales para ese ataque podrían ser nodos o enlaces vitales de información tales como puestos de comando y centros de comunicaciones; posteriormente podrían también golpear la infraestructura de apoyo. Los recursos de apoyo al sistema central tales como fuentes de energía, pueden ser muy difíciles de reparar o reemplazar. Para atacar o golpear, el adversario puede emplear su artillería; sus misiles tácticos y su poder aéreo; cuya precisión estará dada por su habilidad para emplear tecnologías tales como GPS, vehículos aéreos no piloteados e imágenes satelitales en tiempo casi real. Si los SINFOR o instalaciones no pueden destruirse, el adversario podría buscar al menos inutilizarla por el tiempo suficiente para completar su maniobra de acuerdo a sus intenciones.

11. RETOS PARA LA INFRAESTRUCTURA DE INFORMACION Y PARA EL AIM

a. Los Cmdtes y los líderes nacionales enfrentan significativos e interrelacionados retos cuando tratan con la anticipación de los efectos de la visibilidad global de las operaciones y los rápidos cambios en la tecnología de información; y sus impactos en el AIM. Estos retos están

referidos a: la seguridad de la información, la continuidad de las operaciones, políticas y opinión pública, la moral de la tropas y las consideraciones legales.

b. Seguridad de la Información (SEGINFOR)

Dos hechos comúnmente reconocidos direccionan el porque de la seguridad de la información como un reto importante. Primero, los sistemas de inteligencia informan que casi el 95% de las comunicaciones de defensa durante tiempo de paz viajan sobre las redes de conmutación pública relativamente desprotegidas y están grandemente fuera del control directo o influencia de lo militar; y segundo, una cantidad significativa de información y/o inteligencia es transportada por medios comerciales.

c. Continuidad de las operaciones

Debido a la naturaleza dominante, penetrante e impertinente del ambiente de información militar (AIM), la preparación para tratar con las operaciones de información (OI) no debe esperar hasta que una unidad reciba una orden de alerta para desplegarse. Para ese entonces, el Cmdte y su EM deben ya haber desarrollado planes y procedimientos para tratar millares de aspectos e influencias en el AIM o riesgos que rápidamente están siendo sobrepasado por eventos.

d. Política y Opinión pública

(1) Con la visibilidad global, la exposición de información dramática y el análisis de operaciones militares en progreso por expertos (civiles o militares); rápidamente pueden influir en la opinión pública y consecuentemente sobre la política relativa a la conducción de operaciones militares. La población que recibe y potencialmente reacciona, a esta cobertura incluye al publico nacional, los que toman decisiones, los países aliados o simpatizantes y otras naciones neutrales o no. Los medios de comunicación muy probablemente proporcionarán una cobertura de 24 horas de todas las perspectivas, opiniones u análisis sobre las operaciones.

(2) La visibilidad global de las operaciones también puede afectar a los Cmdtes que toman decisiones; ya que cuando la información en el AIG es imprecisa, incompleta, no presentada en contexto, basada en rumores o en el resultado de información con sentido errado o de esfuerzos desinformativos; un Cmdte puede reaccionar apresuradamente, tomando decisiones emocionales o haciendo elecciones que son inconsistentes con la situación real, hasta inclusive optar por la terminación de una operación en curso. Un Cmdte efectivo se anticipa a como un adversario podría intentar manipular los medios noticiosos para prevenir que un potencial enemigo siente o establezca los términos de un conflicto en la arena pública.

e. Moral de las tropas

(1) La visibilidad global de las operaciones impactan sobre la potencia combativa de un comando ya sea mejorando o degradando la moral de las tropas. La perseverancia y espíritu de cuerpo de los soldados; su deseo de ganar; su dedicación a la causa; y, su devoción a sus camaradas de armas y unidad; pueden rápidamente ser indeterminadas por lo que ven en el ambiente de información global e incluso militar.

(2) Las posibilidades de las comunicaciones instantáneas de estos SINFOR a menudo difunden información a los soldados, sea esta precisa o no, más rápido que los canales de comando militares. Noticias malas, malinterpretaciones, información imprecisa, y

desinformación (o información errada); impactan sobre las familias, y pueblos de origen de los soldados y sobre ellos mismos, afectando su moral. De ahí que todo Cmdte debe considerar en su planeamiento los alcances e impacto del AIG sobre la crítica e importante dimensión humana de toda operación, a pesar que la prensa tenga que cubrirlas libremente.

f. Consideraciones legales

(1) Relativamente muy pocas reglas y leyes o normas, gobiernan el empleo o acceso a muchos tecnologías o SINFOR noticiosos. Por esta razón las OI confrontan retos legales y otras restricciones tales como las reglas de compromiso o acuerdo de estatus de las fuerzas.

(2) La tensión existirá tanto en paz como durante períodos de conflicto. La reunión de inteligencia o simplemente la información en tiempo de paz a menudo está limitada por políticas y/o leyes, sin embargo algunas para el uso de sistemas computarizados no militares y otras redes de información en este período, aún no han sido determinadas. Por ejemplo el control o regulación del acceso a internet para proteger información sensible o modos de redes críticas esta mayormente no dirigida ni regulada. Se necesitará una estrecha coordinación con el asesor legal o sistema judicial, para enfrentar los retos de confrontar las operaciones de información con las consideraciones legales.

(3) Debido a que muchos de los protagonistas e influencias en el AIM están fuera del control militar amigo, los contratos o restricciones leales pueden prevenir a los militares de controlar o influenciar el uso de recursos civiles por un adversario. Por ejemplo, durante las hostilidades una fuerza podría depender de una agencia internacional para cambiar su código de acceso para una imagen satelital para proteger información crítica en su zona de responsabilidad, sin el cambio la imagen estaría disponible al mercado abierto; un adversario podría, bajo un contrato comercial, bajar imágenes satelitales críticas de una región geográfica en tiempo casi real conforme un satélite pase sobre una estación terrestre.

SECCIÓN IV. DOMINIO DE LA INFORMACIÓN

12. CONCEPTUALIZACION DEL DOMINIO DE LA INFORMACION

a. El dominio de la información está definido como el grado de superioridad de información que permite al poseedor emplear los sistemas de información y sus posibilidades para lograr una ventaja operacional en un conflicto o controlar la situación en operaciones cortas de la guerra, al mismo tiempo que niega estas posibilidades al adversario.

b. Al igual que se ha venido reconociendo y dependiendo de la superioridad aéroelectrónica como una condición clave para los éxitos militares, el dominio de la información ha tomado una importancia similar para las operaciones militares. Esto significa que el conocimiento amigo y el entendimiento de la situación debe ser más certero, más oportuno y más

preciso que del adversario; revelando a un Cmdte amigo las condiciones que lo llevarán al éxito.

c. La creación del dominio de la información tiene dos facetas igualmente importantes:
   (1) Construir y proteger las posibilidades de información amiga.
   (2) Degradar las posibilidades de información enemiga.

d. La noción de dominio de la información no es nueva. A través de la historia, los Cmdtes han visto apalancar la temporal oportunidad que llega desde una ventaja de información, sea que provenga del conocimiento del terreno o de una imagen satelital.

13. VENTAJA DEL CONOCIMIENTO, LA RESPUESTA A LOS RETOS

a. Los Cmdtes amigos cumplen con el dominio de la información mediante la obtención de la ventaja del conocimiento sobre un enemigo. Esta ventaja es generada por los Cmdtes empleando innovaciones técnicas y procedimientos humanos que permitan a la fuerza más fácilmente capturar y retener la iniciativa total e incrementar su letalidad y supervivencia.

b. Construir una ventaja del conocimiento requiere un sentido altamente desarrollado para saber que información será necesaria y una habilidad para manejar el uso y difusión de ese conocimiento en el lugar y momento correcto para un propósito deseado.

c. Los líderes de éxito usan la ventaja del conocimiento mediante una combinación de la información técnica y humana, con una amplia expresión de su intención y una clara articulación del concepto de operaciones. Semejante al poder aéreo, un Cmdte de fuerzas terrestres puede gozar de un rango de niveles de ventaja del conocimiento desde la supremacía de la información hasta el equilibrio de la información. Un enemigo también puede lograr una ventaja del conocimiento a nuestras expensas.

d. La información puede variar el dominio, cambiando en tiempo y espacio, así como en escalón, un ejército puede alcanzar el dominio de la información en el nivel operacional pero puede perderlo en el nivel táctico.

e. Existen algunas técnicas o procedimientos para lograr la ventaja del conocimiento y que se ampliarán en párrafos separados, esta son:
   (1) Telescopio dirigido.
   (2) Visualización del campo de batalla.
   (3) Conciencia situacional.
   (4) Visión expandida.
   (5) Cobertura abierta de medios.
   (6) Administración de la información.

14. TELESCOPIO DIRIGIDO

a. Las unidades con alto rendimiento son en gran parte distinguidas de las otras unidades por su habilidad para obtener y usar información con efectividad. Históricamente, estas unidades a menudo han logrado la ventaja de la información mediante el empleo de métodos y procedimientos no-tradicionales tal como el denominado "telescopio dirigido".

b. Conceptualmente, el telescopio dirigido adquiere información por medio de la suplementación del flujo de información de rutina, a través de:
   (1) El empleo de canales externos a los tradicionales de comando y su información jerarquizada.
   (2) El uso de unidades de operaciones especiales, oficiales y equipos de reconocimiento y redes especiales de comunicaciones.

c. Estos rendimientos son aún válidos y empleados hoy en día; sin embargo las modernas innovaciones tecnológicas, potencialmente hacen que las ventajas ganadas vía la técnica telescopio dirigido se vuelvan casi rutinaria. Las innovaciones en sensores, procesadores, comunicaciones y computadoras pueden dar a los Cmdtes acceso inmediato a la situación de informaciones amigas y enemigas; y lograr así una subsiguiente ventaja del conocimiento operacional.

15. VISUALIZACION DEL CAMPO DE BATALLA

a. La creación de una ventaja del conocimiento operacional apoyará la visualización del campo de batalla del Cmdte, la misma que está conceptualizada como el proceso por el cual un Cmdte:
   (1) Desarrolla un claro entendimiento de su estado o situación actual en relación al enemigo y al medio ambiente.
   (2) Prevé un estado final deseado que representa la misión a cumplir.
   (3) Visualiza la secuencia de actividades que moverán su fuerza desde su estado actual a su estado final.

b. Un paso clave hacia el logro del dominio de la información será alcanzado cuando el nivel de visualización del campo de batalla de un Cmdte sea significativamente más grande que el de su oponente. En el pasado, el balance o apalancamiento de una ventaja del conocimiento para lograr decisivamente un estado final deseado, ha sido mayormente un proceso intuitivo. Los verdaderos Cmdtes excepcionales casi siempre han poseído este rasgo, al contrario de los menos exitosos. Las tecnologías de la información ahora, mantienen una potencialidad para hacer que estos conocimientos del campo de batalla y sus oportunidades inherentes que ellos ofrecen, sean más accesibles a cada líder de todos los escalones.

c. El efecto de estos retos será el mejoramiento de la visualización del campo de batalla mediante un mejor apoyo a los líderes con procesos de información sistemáticos y deliberados, basados en la construcción de bloques de datos no-procesados analizados sintácticamente y corelacionados por el hombre y la máquina, sintetizados en un todo coherente y enfocado hacia el entendimiento gráfico del caos de batalla.

d. Adicionalmente, mediante el enlace de los Cmdtes en diferentes escalones, está misma tecnología mejorará la conciencia situacional y promoverá el planeamiento y ejecución operacional sincronizados. Idealmente , el Cmdte podrá ver y pensar como uno.

16. CONCIENCIA SITUACIONAL

a. Otro aspecto crítico de lograr una ventaja del conocimiento sobre el adversario es alcanzar una condición de conciencia situacional sobre toda la fuerza. Esta conciencia situacional incluye:
   (1) Un entendimiento común de la evaluación de la situación del Cmdte.
   (2) La intención del Comandante.
   (3) El concepto de operación del Cmdte, combinado con un cuadro claro de los dispositivos y posibilidades de las fuerzas amigas y enemigas.

b. Las operaciones de información potencialmente aseguran la conciencia situacional apropiada a cada nivel de una organización, hasta el soldado individualmente. Los sistemas que hoy en día se están probando en algunas guerras y conflictos, vienen ofreciendo a los Cmdtes un entendimiento colectivo del espacio del batalla. La evaluación de la

situación del Cmdte, su intención y concepto de operación proporcionan el marco que se aplica sobre toda la organización. Este marco fomenta el incremento de la cohesión y unidad de esfuerzo en la ejecución de operaciones. La figura 3 ilustra esta relación.

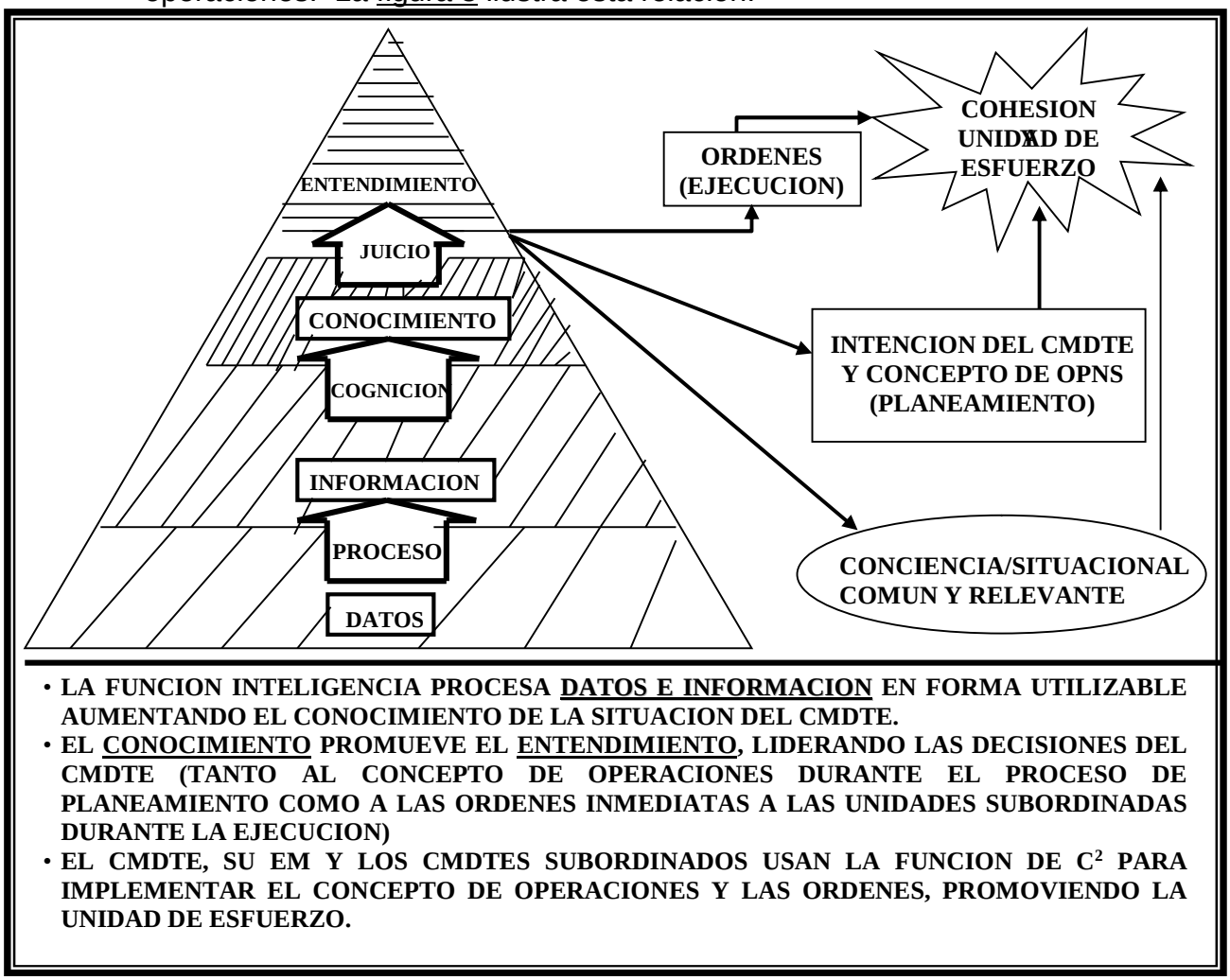

FIGURA 3: CONCIENCIA SITUACIONAL

c. La conciencia situacional es inherentemente local, proporcionando un contexto inmediato y relevante para la interpretación y uso de nueva información conforme es recibida por un soldado en una situación particular. La situación local relevante a cada nivel e individuo es desarrollada dentro de un marco común y compartido vertical y lateralmente como sea apropiado. Esta situación no sólo retiene la ventaja de la estructura jerárquica (intención y marco común) sino también agrega la ventaja de los SINFOR no jerárquicos que posibilitan una acción y adaptación descentralizada para situaciones locales sobre todo el comando.

d. Desarrollando la flexibilidad de una estructura no jerárquica coloca una mayor obligación sobre el Cmdte para articular claramente su intención y concepto de operaciones. Tradicionalmente, los Cmdtes se aseguraban que tanto su intención y el concepto fueran entendidos dos escalones abajo y arriba en una estructura jerárquica; ahora la tecnología de información hace posible que ambas sean, de manera relativa, fácilmente compartidas sobre todo el comando, lo que mejorará el C^2 de la operación cada vez que se haga esto.

e. El arte de comandar requiere establecer claramente un marco común con suficiente libertad para su aplicación y adaptación local. La proliferación de ese entendimiento, potencializa a todos los líderes sobre el campo de batalla, da a la fuerza una perspectiva singular y una claridad de enfocarse en aquello que optimiza su potencia combativa contra un oponente o posibilita controlar una situación en otras operaciones. Negarle al adversario una capacidad similar, tal como degradar su conciencia situacional es un objetivo igualmente importante, que será tratado en el capítulo 3, bajo el título Guerra de Comando y Control (G-C^2).

17. VISION EXPANDIDA

a. La tradicional visión operacional debe expanderse para tomar ventaja total de la potencial contribución de las operaciones de información (OI) para dominar al enemigo al mismo tiempo que se protege a las fuerzas amigas. Antes que cualquier restricción mental sea incluida en la intención o concepto operacional, los Cmdtes de todos los escalones evaluarán aquellos actores y elementos, dentro y fuera de su control, que pueden afectar las próximas operaciones, para incluir aspectos informacionales. El resultado de este proceso de pensar acerca del ambiente de información global (AIG) es un número manejable de elementos informacionales con los cuales un Cmdte decide tratar, los cuales, por definición, lo constituye el AIM para una operación particular. Esto expande la visión del espacio de batalla que puede incluir varias combinaciones de espacio, tiempo, propósito y gente.

b. Los elementos de una visión de OI se alinean con las funciones de combate asociadas con operaciones tradicionales. El AIM, equivalente a la ventaja táctica de poseer terreno elevado o la posición de flanco, podría ser transformado en una ventaja de información de reconocimiento local e internacional. Sólo las maniobras exitosas dan a un Cmdte más opciones que el enemigo; una percepción de credibilidad y apoyo; o una habilidad para comandar y controlar; proporcionando una ventaja para la maniobra informacional. El mantener esta ventaja requiere constante evaluación y ajustes, para el cual se deberá recurrir: a las operaciones sicológicas, a las operaciones de asuntos civiles, evaluación de informes de las organizaciones privadas de voluntarios y a la cobertura de los medios noticiosos; los cuales en conjunto y/o individualmente proporcionarán una forma de reconocimiento y vigilancia, al igual que lo hacen las estandarizadas operaciones de reconocimiento y vigilancia, (OR&V) militares para proveer información que conduce los fuegos y las maniobras subsecuentes.

c. El propósito del poder de juegos en combate es la generación de una fuerza destructiva contra las posibilidades enemigas y su voluntad de lucha. El ambiente de información militar (AIM) al igual que el poder de juegos, es el empleo de las posibilidades letales o no, y directas o indirectas a través de la guerra de comando y control (G-C^2).

d. La G-C^2 usa las operaciones de engaño, las operaciones sicológicas, la guerra electrónica y la destrucción física; para atacar las posibilidades de un adversario, al mismo tiempo que protege las operaciones amigas. La integración de la G-C^2 a las tradicionales operaciones tácticas, aumenta la precisión del proceso de selección de objetivos mediante la dirección del poder de los tradicionales ataque, engaño, operaciones sicológicas, GE y SEGOPE (seguridad de las operaciones) en el ciclo de decisión del

adversario, para así ganar el control del mismo y ayudar a generar dominio de la información.

e. Los últimos conflictos armados han mostrado y así lo han reconocido los ejércitos modernos; que la cobertura de los medios noticiosos impacta sobre el propósito, naturaleza y duración de las operaciones mayores y que también el AIG afecta las operaciones en los niveles división y menores (inclusive hasta nivel compañía). Los Cmdtes hoy en día, en cada escalón de comando; deben continuamente manejar cuidadosamente la separación de las funciones de relaciones públicas y operaciones sicológicas, para preservar la integridad y credibilidad de las operaciones civiles - militares. Los métodos para emplear de manera integrada la G-C^2, las relaciones públicas y las operaciones civiles militares, para mejorar las operaciones tácticas es tratado en el Cap.3.

f. Las actividades que afectan el como son vistas y percibidas las operaciones por diferentes audiencias están en frecuente crecimiento y requieren que sean calculadas por un comando de batalla, siendo un prerequisito para una efectiva visualización del espacio de batalla. El requerimiento para identificar y calcular las audiencias críticas, los mensajes y los medios de comunicaciones no es nuevo para los líderes; sin embargo en la guerra moderna a cobrado una mayor significación para el éxito de las operaciones.

18. COBERTURA ABIERTA DE MEDIOS

a. Además de reforzar a una visión más amplia del ambiente, las operaciones de información implican una atención especial a los medios noticiosos y a la visibilidad global de las operaciones. La política de gobierno y del sector defensa en particular, determinarán los principios que regirán la cobertura noticiosa de combate por los cuales los Cmdtes del ejército se guiarán, teniendo en cuenta que proporcionar una cobertura abierta e independiente a los medios de comunicación puede proporcionar a la opinión pública nacional una visión compartida y de influencia positiva a favor del empleo de sus fuerzas armadas y sus posibilidades; si es que las OI son adecuadamente conducidas. Esta política debe dar a los Cmdtes y líderes en todos los escalones una misión clara para preparar con efectividad a las tropas para tratar con los medios noticiosas, antes, durante y después de todas las operaciones.

b. La principal herramienta de un Cmdte de división y Cmdtes de elones superiores para tratar con los medios de comunicación son las relaciones públicas, las que direccionarán los asuntos que integran a todos los niveles de la guerra. Sin embargo, a escalones menores a división, el Cmdte no tiene un oficial de EM especialmente a cargo de esta responsabilidad; a pesar que a menudo las unidades, destacamentos y/o agrupamientos deben alojar, apoyar y acompañar a reporteros, enviados especiales y/o corresponsales de guerra. Los Cmdtes deben entender y entrenar a sus soldados así como ellos mismos, el plan para el manejo y presencia de los medios noticiosos, proveyéndoles entrevistas efectivas que comuniquen información legitima al público, orientado a fortalecer la moral y la cohesión de la unidad, al mismo tiempo que mejore su habilidad para cumplir su misión.

c. Aunque la intención clara de lo expuesto hasta el momento es requerir que los Cmdtes presten especial atención a los medios y a su potencial impacto sobre las operaciones militares; es claro también que los conceptos doctrinarios discutidos en este manual no sancionan en ninguna forma las

acciones que se intenten para inducir a error o manipular a los medios que cubren las operaciones militares. Por el contrario, el ejército acepta y endosa totalmente la sana tensión que existe entre el deseo normal de los medios para informar al público tanto como sea posible sobre esas operaciones militares; y el deseo normal de los Cmdtes para controlar el ambiente de la información sobre aquellas mismas operaciones en el grado más alto posible.

19. ADMINISTRACION DE LA INFORMACION

a. La administración de la información toma una importancia creciente para enfrentar los retos de la visibilidad global, del rápido cambio de la tecnología de la información y de su impacto sobre el AIG. El reto de obtener miles de datos y transformarlos rápidamente en conocimiento y entendimiento, requiere un proceso cíclico y continuo donde la toma de decisiones viene incrementando su dinamismo y multidimensionalidad. Las decisiones sobre las operaciones en curso deben ocurrir simultáneamente con las decisiones y el planeamiento de operaciones futuras. La toma de decisiones debe enlazar perfectamente la paz con los cambios de la conciencia situacional .

b. La tecnología de la información permite ahora el movimiento horizontal y la integración de información y proporciona un marco para la toma de decisión local, permitiendo potencialmente que el alcance de control del Cmdte aumente sin pérdida de eficiencia. El dinamismo de las operaciones modernas afecta de manera crítica el alcance de control del Cmdte, debido a que un moderno campo de batalla presenta a los fuerzas separadas crecientemente, dejando grandes espacios entre formaciones y requiriendo que cada grupo de fuerzas actúen con gran autonomía sin expandir la zona de operaciones. La dispersión crea más grupos de fuerzas subordinadas, descentralización de la autoridad de decisión y mayor necesidad por esfuerzos coordinados. El alcance de control nominal será incrementado y la conciencia situacional total será más complicada.

c. El saber aprovechar la potencialidad de la información para transformarla a como el ejército opera será crítico para sus éxitos en el futuro. Sin embargo, la tecnología por sí sola no puede proporcionar a los líderes: con una visualización del campo de batalla de manera automática, con una conciencia situacional perfecta, con una visión expandida fácilmente o con una administración de la información altamente efectiva. Al final del análisis, el producto de la iniciativa para aprovechar la potencialidad de la información solo podrá apoyar: la aplicación del buen juicio de un líder, su sabiduría, su experiencia y su intuición; para mejorar su comando de batalla.

d. UN INCREMENTO DE LA CANTIDAD DE INFORMACION DISPONIBLE NO GARANTIZA SU CERTIDUMBRE; DE HECHO, SU AMBIGUEDAD PUEDE POTENCIALMENTE INCREMENTARSE. LOS METODOS ANALITICOS, LOS PROCEDIMIENTOS Y ORGANIZACION DE UN ESTADO MAYOR ACTUAL, DEBEN AJUSTARSE PARA LLEGAR A DOMINAR LA RIQUEZA DEL FLUJO, EL PASO RAPIDO Y EL ALTO VOLUMEN DE INFORMACION. EL MAYOR RETO SERA ENCONTRAR LOS MEJORES PROCEDIMIENTOS DE ANALISIS Y TOMA DE DECISIONES Y NO SOLO LOS MAS RAPIDOS.

CAPITULO 2
FUNDAMENTOS DE LAS OPERACIONES DE INFORMACION

SECCIÓN I. NATURALEZA DE LA INFORMACION

20. JERARQUIA COGNOCITIVA

a. Este capítulo da una idea general de la naturaleza de la información y los fundamentos de las OI exponiéndose que son, que aplican y como se relacionan sus diversas actividades. Discute además los componentes de las OI: operaciones; información relevante e inteligencia; y sistemas de información (SINFOR). Se concluye con una discusión de las seis (06) actividades críticas y esenciales para un programa de OI sensato: obtención, empleo, protección, explotación, negación y manejo de la información y SINFOR.

b. Dentro de lo que constituye la naturaleza de la información, existen dos conceptos importantes que son necesarios introducir: la jerarquía cognocitiva y la guerra de información. En este párrafo se desarrolla en detalle el primero de ellos.

c. La jerarquía cognocitiva parte de la idea que un pedazo o porción de dato dado, mayormente no tendrá sentido por sí mismo; sólo cuando dicho dato es procesado se colocará en un contexto situacional, ganando significado y llegando a ser por definición información.

d. De la información se deriva el conocimiento, que es información que ha sido probada y aceptada como objetiva o que se atiene a los hechos mediante:
   (1) La cognición, es decir el proceso mental que recibe o desarrolla información no verificable (creencia, opinión, convicción)
   (2) La evaluación o test para probar la información.
   (3) La aceptación de la información como un hecho factual.

e. Los Cmdtes y sus planificaciones (EEMM) siempre deben ser sensitivos para diferenciar entre creencias y conocimiento. Las creencias no probadas, aun cuando sean comúnmente aceptadas, se diferencian de los hechos y son en esencia opiniones que más adelante podrían probarse como erradas. Las decisiones que se basen en creencias en lugar de hechos son siempre un riesgo.

f. Del conocimiento se deriva el entendimiento, que será alcanzado por el empleo de algún juicio que de al conocimiento relevancia dentro de un contexto situacional específico. Idealmente, el entendimiento de una situación apoyará al comandante en su visualización del campo de batalla y creará las condiciones desde las cuales los planes pueden formarse y tomarse acciones efectivas. En la figura 3, se mostró la pirámide o jerarquía cognocitiva y su relación dentro de la conciencia situacional.

g. Si bien es ciertamente deseable alcanzar un entendimiento total de una situación antes de tomar decisiones, los Cmdtes deben estar totalmente preparados para tomar decisiones en un ambiente operacional de ambiguedad, caracterizado por información imperfecta y entendimiento incompleto. La toma de decisión de un comando seguirá siendo más un arte que una ciencia aún en la era de la información. En todo caso la meta de las OI será acortar o estrechar la distancia entre el arte y la ciencia de la toma de decisión de un comando.

21. GUERRA DE INFORMACION (G-I)

a. Las fuerzas armadas modernas reconocen que la guerra de información es una de las muchas posibilidades del poder nacional de los elementos militares de una nación. La G-I puede apoyar toda una estrategia de gobierno como política de lucha; durante tiempo de paz, crisis, conflicto y post conflicto. La habilidad de un país para influir las percepciones y toma de decisiones de otras países impacta grandemente la efectividad de disuación, influencia sobre naciones con poder y otras conceptos estratégicos.

b. La G-I está definida como las acciones tomadas para alcanzar superioridad de información mediante la afectación de la información del adversario, de sus procesos basados en información, de sus sistemas de información y de las redes basada en computadoras; defendiendo simultáneamente nuestros mismos procesos, sistemas, redes e información.

c. La G-I si esta cuidadosamente concebida, coordinada y ejecutada; puede:
   (1) Contribuir a distender crisis.
   (2) Reducir el período de confrontación y mejorar el impacto de los esfuerzos informativos, diplomáticos, económicos y militares.
   (3) Anticipar o eliminar la necesidad para emplear fuerzas de combate.

d. El Objetivo de la G-I es conseguir una ventaja de información significativa que posibilite a la fuerza en su conjunto, dominar y controlar rápidamente al adversario. La meta estratégica de la G-I es capturar y mantener una ventaja decisiva mediante el ataque a la infraestructura de información nacional (IIN) del adversario a través de su explotación, negación e influencia; al mismo tiempo que se protege los SINFOR amigos. La G-I ofrece a ambos contendores la oportunidad para golpear a distancia con relativa seguridad.

e. La G-I está mas orientada al impacto de la información sobre todo un país durante un conflicto en curso; sin embargo a nivel ejército el concepto de G-I está tomado en un contexto más amplio para orientarlo al impacto de la información sobre las operaciones terrestres en todo el rango de ellos y desde época de paz hasta la guerra total. A esta concepción ampliada de la G-I se le denomina OPERACIONES DE INFORMACIONES (OI), que implementa las políticas de la G-I para un Cmdte del componente terrestre.

f. LA OI están definidas como las operaciones militares continuas dentro del AIM que posibilita, mejora y protege la habilidad de las fuerzas amigas para reunir, procesar y actuar sobre la información para alcanzar una ventaja a través de todo el rango de la operaciones militares; incluyendo la interacción con el AIG y la explotación o negación de información y posibilidades de decisión de un adversario. Las OI integran todos los aspectos de la información para apoyar y mejorar los elementos del poder de combate (potencia combativa), con el objetivo de dominar el espacio de batalla en el momento y lugar correcto; y con las armas y recursos apropiados. Las unidades conducen OI a través de todo el rango de las operaciones militares, desde las operaciones en guarnición en época de paz, pasando por el despliegue, las operaciones de combate y continuando hasta el redespliegue y completamiento de la misión. En la siguiente sección se describirán sucintamente los componentes de las OI.

SECCION II. COMPONENTES DE LAS OPERACIONES DE INFORMACION

22. ASPECTOS INTRODUCTORIOS DE LOS COMPONENTES DE LAS OI

a. Las actividades que apoyan a las OI incluyen:
   (1) Obtención de información y SINFOR.
   (2) Empleo de información y SINFOR.
   (3) Manejo de información y SINFOR.
   (4) Explotación de información y SINFOR.
   (5) Negación de información y SINFOR.

b. Estas actividades tomar lugar dentro de los tres (03) componentes de las OI:
   (1) Operaciones de información propiamente dicha.
   (2) Información relevante e inteligencia (IRI).
   (3) Sistemas de información (SINFOR)

c. Estos componentes operan dentro de un espacio de batalla establecido por el AIM, tal como se muestra en la figura 4, operaciones de información. Las organizaciones del ejército deben conducir estas actividades de las OI como parte de un dinámico proceso iterativo para apoyar cada componente en una operación integrada y totalmente dimensionada.

d. En esta sección se describirán brevemente los componentes de las OI y en la siguiente sección las actividades que se integran a ellas y las apoyan.

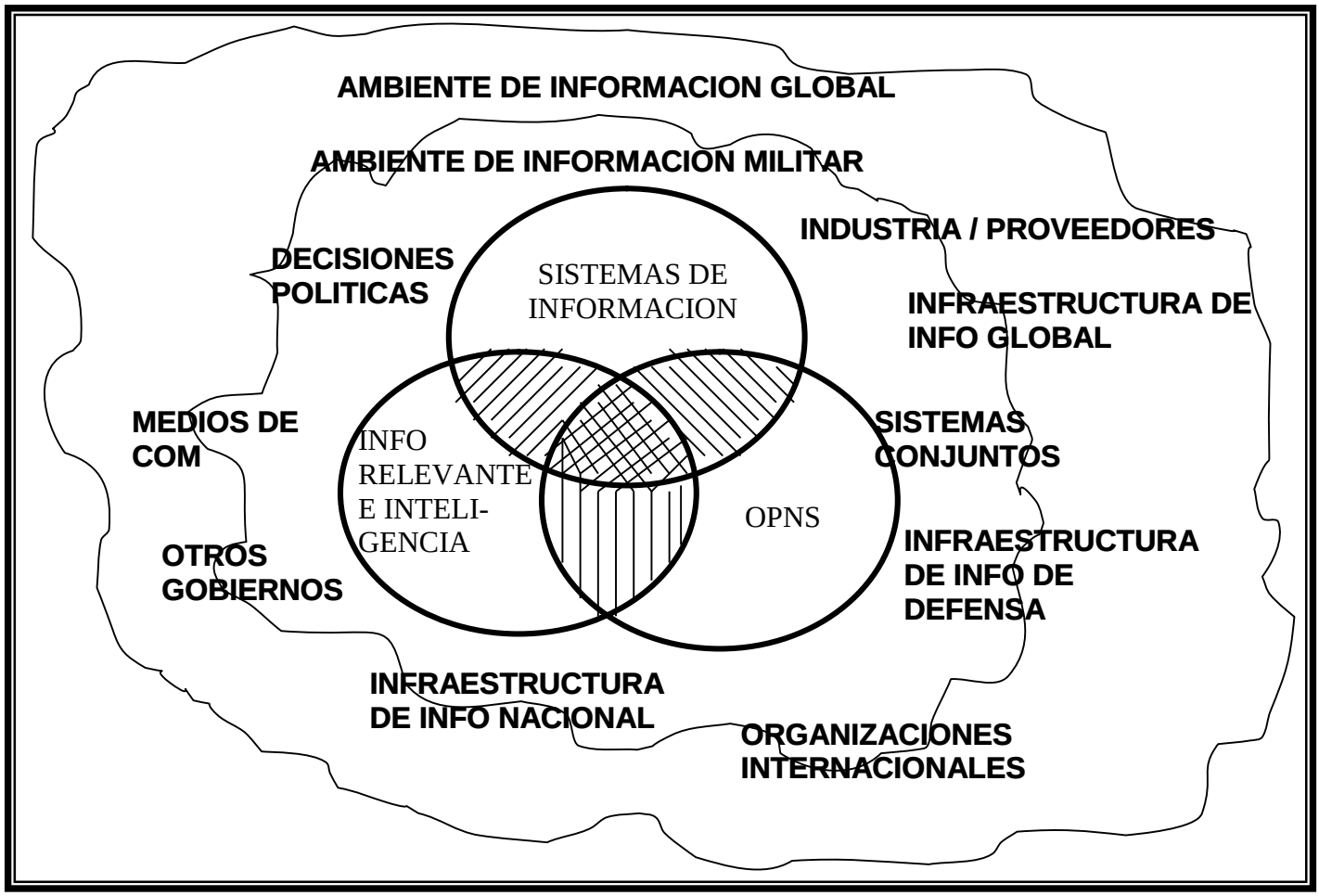

FIGURA 4: OPERACIONES DE INFORMACION

23. OPERACIONES DE INFORMACION PROPIAMENTE DICHA

a. Para ganar y mantener el dominio de la información y un efectivo C^2, el ejército deberá emplear tres (03) operaciones específicas:
   (1) Guerra de comando y control (G-C^2)
   (2) Operaciones civiles - militares (o asuntos civiles: AC)
   (3) Operaciones de relaciones públicas (RP).

b. Estas tres operaciones están interrelacionadas y se conducen para apoyar el objetivo del ejército de alcanzar el dominio de la información en cualquier ambiente operacional, en paz o en combate. Cada una de estas operaciones pueden igualmente contribuir al éxito de cualquier misión; una proporcionará al Cmdte posibilidad de combate tradicional (G-C^2), mientras las otras (AC y RP) apoyarán el combate y proveerán enlace esencial a la creciente influencia del AIG.

c. Dependiendo de la situación, la G-C^2, los AC y los RP; jugarán un rol importante en operaciones de paz y de combate, cuando establezcan y mantengan el dominio de la información y colectivamente den al Cmdte las herramientas para definir y controlar el ambiente de la información. Será necesario que el Cmdte en cada situación balancee estas operaciones para alcanzar su objetivo.

d. Al agrupar estas tres operaciones específicas bajo un mismo concepto de operaciones, lo que se busca es dar un marco que promueva la sinergia y facilite el planeamiento y ejecución de un EM, proporcionando además una mayor integración y sincronización de las operaciones de AC y RP con los elementos más tradicionales de combate de la G-C^2.

e. En los párrafos siguientes se desarrollan sucintamente estas tres operaciones específicas y en capítulo posterior se trata con mayor profundidad lo referente a la G-C^2.

24. OPERACIONES DE GUERRA DE COMANDO Y CONTROL (G-C^2)

a. La G-C^2 es la aplicación combativa de la G-I en operaciones militares. El objetivo de la G-C^2 es influir, negar información, degradar o destruir las posibilidades de comando y control del adversario; mientras protegemos las nuestras contra tales acciones.

b. El planeamiento de la G-C^2 es conducido sobre todo el continuo operacional militar, desde época de paz hasta la culminación de las hostilidades. En el pasado, el principal objetivo del combate fue concentrar potencia combativa física y destructiva contra el personal y el equipamiento adversario, esto es, tanques, aeronaves, artillería y defensa aérea. Posteriormente a comienzos de la década de los 90's nuestro ejército incorpora la doctrina americana de la batalla aeroterrestre que incluía este pensamiento mediante el enlace de operaciones aéreas y terrestres para alcanzar profundidad y sincronización. Un parámetro consecuente de la doctrina de la batalla aeroterrestre fue la intención de golpear a las reservas, los refuerzos y fuerzas del segundo escalón. Actualmente a la luz de la experiencia de las guerras y conflictos de los últimos 10 años, la estrategia operacional se ha extendido a las operaciones en profundidad con armas de largo alcance y operaciones de fuerzas especiales; buscando objetivos de alto valor con una estrategia orientada a la destrucción, degradación, negación y dislocación de nodos de C^2 críticos como uno de sus objetivos principales.

c. Para lograr la estrategia de las operaciones en profundidad, hoy en día las operaciones de G-C^2 integran y sincronizan las posibilidades de las operaciones sicológicas, el engaño, la seguridad de las operaciones (SEGOPE) y la guerra electrónica; para facilitar la aplicación de fuerzas y sistemas apropiados y para ejecutar las operaciones de información. Aunque en el pasado la G-C^2 ha tenido como su principal foco la ofensiva bajo la denominación de estrategia de contramedidas de comando, control y comunicaciones (CMC^3) (Ver manual de Seg. de Com. Ed. 1998 y Empleo Táctico de GE Ed. 1998),ahora incluye también aspectos de protección; constituyendo los dos componentes o disciplinas principales de la G-C^2:
   (1) Ataque de comando y control (Ataque - C^2).
   (2) Protección de comando y control (Protección - C^2).

d. En realidad en la práctica estas dos disciplinas de la G-C^2, han sido empleadas por ejércitos victoriosos desde que la historia empezó a registrarse; sin embargo en la guerra moderna con su énfasis sobre las informaciones y sistemas de información requiere una perspectiva nueva. Para ello será necesario tener en cuenta tres factores que hacen que las consideraciones de la G-C^2 sean críticas cuando se opera en un ambiente actual, estos factores son:
   (1) El contínuo, como resultado del alto volumen del flujo de información dictado por la relación de la tecnología militar moderna y las operaciones militares.
   (2) Las vulnerabilidades que se crean con la incorporación generalizada de tecnología avanzada para los sistemas de información e inteligencia.
   (3) El radical mejoramiento de las posibilidades de los SINFOR y de la inteligencia como resultado de los explosivos avances en la tecnología.

e. La complejidad y el alcance del AIM de hoy, incrementa la dificultad de alcanzar una desorganización, desarticulación y/o dislocación comprensiva de las posibilidades de C^2 adversario mediante algún ataque singular o aplicación del poder de combate. Esto realza la importancia de una efectiva integración y sincronización de los cinco elementos de la G-C^2: la guerra electrónica, el engaño, las operaciones sicológicas, la SEGOPE y la destrucción física; para lograr resultados máximos cuando se lancen ataques. Muy probablemente también se requerirá de una cuidadosa integración y sincronización para una total protección de nuestros SINFOR e inteligencia críticos, contra los ataques del adversario. Sin la completa y total integración de los cinco elementos de la G-C^2 en las dos disciplinas o componentes de la misma, la eficiencia operacional será reducida y las potenciales vulnerabilidades expuestas al eno.

f. Las disciplinas o componentes, así como los elementos de la G-C^2 son ampliamente discutidos en el capitulo 3, sin embargo a manera de introducción se describirán brevemente sólo los componentes:
   (1) Ataque de C^2 (Atq'-C^2)
      (a) El objetivo de la G-C^2 ofensiva o ataque de C^2, es ganar el control sobre las funciones de C^2 del adversario, tanto en términos de flujo de información como en nivel de conciencia situacional. Con un efectivo ataque de C^2, se podrá tanto prevenirse de un adversario por el ejercicio efectivo de nuestro C^2 o nivelándolo o apalancándolo a nuestro favor o ventaja.

(b) El ataque -C^2 puede golpear las posibilidades adversarias en todos los escalones, tomando como objetivos al personal, equipo, comunicaciones y facilidades, en un esfuerzo para dislocar o darle la forma que deseáramos al C^2 adversario.

(c) La información relevante e inteligencia (IRI) juegan un rol clave en el ataque -C^2 con la creación y mantenimiento de bases de datos en cada región militar sobre personal, sobre influencias históricas y culturales, preparación de inteligencia del campo de batalla (PIC) y evaluación de daños de batalla. El problema principal de la ataque -C^2 para influir sobre el C^2 adversario es la aplicación sincronizada de las seis actividades de la información.

(2) Protección de C^2

(a) Las operaciones de protección -C^2 buscan mantener un comando y control efectivo de las fuerzas amigas mediante la negación o tomándola en ventaja amiga de los esfuerzos adversarios; para influir, degradar o destruir los sistemas de C^2 amigo.

(b) La protección -C^2 esta dividido en medidas activas y pasivas que buscan limitar las vulnerabilidades de las fuerzas (en personal, equipo e información) a la acción hostil, aún cuando las fuerzas desplegadas enfrentan amenazas sobrexpandidas y posibilidades adversarios.

(c) La protección -C^2 incluye contrarrestar una propaganda adversaria para prevenirse que puedan afectar las operaciones amigas, sus opciones, la opinión pública y la moral de las propias fuerzas.

25. OPERACIONES DE ASUNTOS CIVILES (AC)

a. Los AC apoyan a los OI proporcionando un rol integral de interface con los actores o protagonistas e influencias en un AIG. Ya sea en paz, conflicto o guerra, la conducción de las operaciones militares, la consolidación de la potencia combativa y la búsqueda del dominio de la información; son mejoradas cuando se balancea con el apoyo de los AC. Aunque las condiciones difieren a través del espectro de conflictos, las actividades de AC establecen, influencian o explotan las relaciones entre las fuerzas militares, las autoridades civiles y la población civil en una zona de operaciones para facilitar las operaciones; creando un intercambio de informaciones que promueven el entendimiento, la confianza y la percepción positiva de las medidas que soportan las operaciones militares.

b. Podría ser necesario el establecimiento de un centro de operaciones civiles-militares (COCM), para que en él interactuen los actores claves e influencias en el AIG. Los elementos de AC apoyan a las operaciones militares mediante la aplicación de su habilidad y experiencia en temas de administración pública, economía local, facilidades públicas, traducciones, traducciones e interpretaciones lingüísticas, relaciones culturales e información civil; así como cualquier información que se reuna y que sea relevante para satisfacer las necesidades de información crítica del comandante (NICC).

c. El personal de AC tiene un rol intricado e importante en la provisión de información durante los ciclos de inteligencia y planeamiento operacional. Los Cmdts incluyen operaciones de AC en su orientación del planeamiento y los planificadores de AC deben considerar toda la información y apoyo

disponible para asegurar el completamiento exitoso de una misión de AC. De existir unidades de AC, estas deben estar bien organizadas y conformadas para planear, coordinar, apoyar y si fuera necesario dirigir y supervisar, varias operaciones para apoyar los objetivos del Cmdte.

26. OPERACIONES DE RELACIONES PUBLICAS (RP)

a. Muchas operaciones militares son conducidas bajo la mirada atenta del escrutinio público. La cobertura de los medios noticiosos nacionales e internacionales juegan un rol importante en la rápida formación de debate y opinión pública. Los medios de comunicación sirven como un foco público para el análisis y critica de las metas, objetivos y acciones; pudiendo impactar en el planeamiento político, estratégico y operacional, en las decisiones y en los éxitos o fracasos de la misión.

b. La existencia de información en tiempo casi real, procesada y trasmitida a grandes velocidades y para audiencias más amplia que en el pasado; han "puenteado" el espacio entre lo que ocurre sobre el terreno y las metas y objetivos de la estrategia militar y/o nacional. Por eso, los Oficiales de relaciones públicas deben monitorear las percepciones públicas, desarrollando y difundiendo mensajes claros y objetivos sobre las operaciones militares. Más aún, los mismos Cmdtes deben involucrarse también en esta dimensión de las OI.

c. El personal que trabaja en RP debe:
   (1) Asesorar al Cmdte trabajando para establecer las condiciones que lideren la confianza y el apoyo al ejército.
   (2) Apoyar abiertamente, informando independientemente y accediendo a los unidades y tropas.
   (3) Buscar una balanceada presentación creíble e imparcial de la información que comunique la versión del ejército, a través de un flujo de información expeditivo, completo, preciso y oportuno.

d. El Cmdte usa su programa de información interna para comunicar a sus tropas sobre donde ellos se colocan, que se espera de ellos y como ellos ayudarán a cumplir la misión. Está comunicación también ayudará a contrarrestar los efectos de la propaganda enemiga o malinformación sobre las tropas que combaten. El Cmdte, mediante su oficial de RP; inicia , dirige y enfatiza los tópicos y programas de información interna; de tal manera que cada soldado reciba información específica de la operación a través de los canales de comando y medios locales, nacionales y mundiales. Los medios son un canal de información importante para el público nacional, sin embargo los Cmdtes, los oficiales del EM y los soldados deben balancear la seguridad de las operaciones (SEGOPE) y otros requerimientos operacionales cuando trabajen con los medios.

e. Los lideres deben integrar las RP en sus procesos de toma de decisiones, considerándolo en sus evaluaciones de la situación y en el desarrollo de formas de acción, planes y órdenes. Los Cmdtes deben asegurarse que las operaciones de RP estén sincronizadas con otras funciones de combate y promover la temprana coordinación de las funciones de RP, AC y operaciones sicológicas durante el proceso de planeamiento. Igualmente deberá existir un continuo intercambio de información durante la ejecución.

27. INFORMACION RELEVANTE E INTELIGENCIA (IRI)

a. Los líderes a través de la historia han luchado contra las dificultades de como capitalizar mejor la información disponible. El llegar a saber tanto como sea posible sobre sus propias fuerzas (ubicación, eficiencia, combativa y actividades actuales) y las del enemigo (ubicación, dispositivo, eficiencia combativa y acciones que intenta), ha sido una característica perdurable de los Cmdtes exitosos. Hoy en día, los Cmdtes operan en un ambiente marcadamente incrementado por flujos de información y decisiones rápidas en todos los niveles (estratégico, operacional y táctico). Estos factores se han complicado por la explosiva expansión en las oportunidades de acceso y por la manipulación de información relevante operacionalmente, debido al amplio arreglo de individuos, organizaciones y sistemas encontrados en el AIG.

b. Finalmente, un C^2 efectivo es dependiente de que se asegure que la persona correcta tenga la información correcta en el momento oportuno. La inteligencia, como fuente de información relevante del Cmdte sobre el adversario, ha tomado una importancia creciente y crucial en la era de la info. La inteligencia sobre los adversarios actuales o potenciales debe ser preparada sobre una escala global, debido a que las OI permiten dar al espacio de batalla, una conectividad global. La interacción con el AIM requiere de inteligencia oportuna sobre muchas aspectos de los adversarios actuales o potenciales, incluyendo los referidos a la cultura, la política y el comercio.

c. Para comandar los Cmdtes deben tener información, ya que esta le permitirá a su ciclo de decisión y ejecución funcionar y dar dirección a las acciones de la fuerza para cumplir sus misiones operacionales.

d. La reunión, procesamiento y difusión de información relevante es la clave para alcanzar conciencia situacional sobre toda la fuerza, creando la oportunidad para la unidad de esfuerzo orientado al cumplimiento de la misión. El Cmdte opera dentro del AIG, ajustando su AIM para mejorar su conciencia situacional como sea apropiado para la operación en curso.

e. El Cmdte se concentra sobre sus necesidades de IRI, que dirigirán sus NICC, las cuales a su vez orientarán el esfuerzo de búsqueda de IRI . Para que sea efectivo, el ciclo de inteligencia de la unidad debe ser manejado para proveer información basada en las prioridades del concepto de operaciones; para lo cual, la clave para las OI exitosas será una precisa PIC enfocada en el AIM. Durante las operaciones de combate, el analista de inteligencia debe continuamente realizar una evaluación de daños de batalla orientado a la información para asegurar que las OI continúan siendo efectivas. El apoyo de la IRI a las OI comienza desde época de paz y debe continuar sobre todas las fases de una operación o campaña.

f. Los avances en la tecnología de la información están mandatoriamente cambiando en como será proporcionado el apoyo de IRI. Primero, la conectividad de las comunicaciones permite una amplia difusión de información, incluyendo enlaces de bajada directos (Vía satelite) de ráfaga de datos desde múltiples sensores a múltiples escalones simultáneamente; y segundo, la radiodifusión de productos de información finales desde dependencias o entidades nacionales de defensa y de las propias fuerzas del ejército desplegadas, proporcionan otras fuentes de info.

g. Las OI requieren de la fusión de información proveniente de una variedad de fuentes. Los avances en sensores, procesadores y comunicaciones, se combinan para proporcionar reconocimiento y vigilancia (R&V) detallada y oportuna de casi cualquier lugar sobre el planeta; y aunque dichos avances no están aún al alcance de nuestro país, los tratados, alianzas, pactos y convenios con países desarrollados poseedores de esta tecnología e inclusive contratos con proveedores, fabricantes o industrias de estos artefactos; nos pueden dar una vía de como aprovechar esta posibilidad. Las fuentes militares y no - militares proporcionan información que puede emplearse para producir IRI. Los informes e inteligencia de fuente abierta proporcionarán muchos de los datos técnicos y de orden de batalla, orientado al comando, control, comunicaciones, computación e inteligencia (C^4I), incluyendo datos de sistemas de reunión y procesamiento de información, sistemas de comando y sistemas de reconocimiento, inteligencia, vigilancia y adquisición de blancos.

h. La integración exitosa de las OI requiere una PIC fundada en un total entendimiento de las posibilidades adversarias y de su estilo de tomar decisiones. Una PIC basada en el enfoque del C^4 I sobre una decisión de necesidades del adversario. Estas son seleccionadas en relación a las necesidades prioritarias de inteligencia (NPI) del Cmdte y describen en detalle las decisiones que el adversario debe tomar para conducir su plan de batalla. Desde ahí, el enfoque se desplaza a las fuentes de información que sostienen o influencian las decisiones tales como los sensores, los radares y sus sistemas de comando, control y comunicaciones (C^3) que les apoyan. El resultado debería incluir datos sobre las operaciones actuales, sus posibilidades y vulnerabilidades.

i. La IRI como un componente de las OI es tratada en detalle en el Cap. 4.

28. SISTEMAS DE INFORMACION (SINFOR)

a. Los SINFOR reúnen, procesan y difunden información relativa a las operaciones actuales y futuras. La automatización ha hecho grandes avances en el procesamiento de la información, pero el hombre sigue siendo el sistema más efectivo para determinar la relevancia de la información.

b. Los SINFOR son aquellos medios que posibilitan al Cmdte y a su EM lo siguiente:
   (1) Monitorear la situación actual.
   (2) Sincronizar las operaciones.
   (3) Integrar y sincronizar las operaciones a través de los sistemas operaciones del campo de batalla (SOC's).
   (4) Coordinar el apoyo naval y aéreo conjunto.
   (5) Actualizar los parámetros de los objetivos de sistemas de armas.
   (6) Controlar las operaciones estrechas, profundas y de retaguardia como si fueran una sola operación.

c. Arquitectura de los SINFOR.
   (1) Los SINFOR son esenciales para la aplicación efectiva del poder militar. Una arquitectura integrada del ejército de los SINFOR, maximizará las posibilidades de C^2 de las fuerzas terrestres en todos los ambientes operativos. Por ejemplo, el Instituto Geográfico Nacional (IGN) puede ser la base para el desarrollo no sólo de cartas

digitalizados, sino también para mapas de carreteras, entregando productos en disketts o CD's , para integrarles en terminales tácticos (TACTER) que mejorarían las operaciones del ejército.

(2) En la actualidad, aún hay mucho por hacer para integrar, y digitalizar todos los SINFOR del ejército, desde la implementación de los sistemas de C^4I hasta la creación de un ambiente operativo común conjunto de sistemas interactivos y estandarizados con plantillas computarizadas para la reunión, almacenaje y manipulación de todas las base de datos. Constituye un reto para comunicaciones, en especial para sus elementos informáticos, la creación, el desarrollo y la evolución de una arquitectura de información comprensiva del ejército, que vise la creación e integración de las arquitecturas operacionales, de sistemas y técnicas:

(a) Arquitectura Operacional
Está arquitectura establecerá la conectividad requerida entre procesos, funciones, información y organización; que muestre que debemos hacer, que información necesitamos hacer y que tan a menudo necesitamos intercambiar información dentro de la fuerza.

(b) Arquitectura de Sistemas
Está arquitectura buscará identificar las relaciones entre los componentes de los sistemas C^4I y crear conectividad física dentro del sistema de información; empleando un contexto organizacional que muestre la distribución del sistema y los estructuras de red, y que ayude a documentar la ingeniería de las decisiones, tales como protocolos de información específica y anchos de banda.

(c) Arquitectura Técnica
Esta arquitectura establecerá un juego de reglas que gobiernan los arreglos, interacciones e interdependencias de todas la partes y elementos que juntos constituyen nuestros SINFOR; especificado los estándares permisibles para el diseño de las posibilidades del C^4I.

d. Integración
La integración de los SINFOR, tanto vertical como horizontalmente, facilitará las consideraciones tácticas y operacionales básicas de: agilidad, iniciativa, profundidad, sincronización y versatilidad; que serán esenciales para los éxitos del ejército en operaciones conjuntas y combinadas.

e. Conectividad global

(1) La conectividad global es esencial para enlazar los aspectos tácticos, operacionales y estratégicos de las OI y para la habilidad de tener la capacidad para actuar en cualquier parte del territorio nacional en cualquier momento. Los SINFOR apoyan a la globalización de las opns con arquitecturas de comunicaciones automatizadas (terrestres, inhalámbricas y/o satelitales) tanto militares como comerciales.

(2) El reto hoy en día es digitalizar todas los sistemas de comunicaciones del campo de batalla, para que se pueda proporcionar C^2 que fluya a través de cada nivel de operación o de guerra. El proceso de migración probablemente dependerá de las disponibilidades presupuestarias y financieras del ejército, pero un proceso por etapas podría ser una solución, para crear un sistema de comando de batalla del ejército. Este sistema que deberá integrar modernos SINFOR con

las unidades tácticas, mejorará la conectividad, el proceso de toma de decisiones, la letalidad, la supervivencia y la habilidad para controlar el ritmo de las operaciones.

f. En el capitulo 5, se discute con mayor detalle la arquitectura de los SINFOR y otros temas que se le relacionan.

SECCION III. ACTIVIDADES DE LAS OI

29. ASPECTOS INTRODUCTORIOS DE ACTIVIDADES DE LAS OI

a. Como se ha manifestado las actividades de las OI son seis e incluyen:
   (1) Obtención de la info y SINFOR.
   (2) Empleo de la info y SINFOR.
   (3) Protección de la info y SINFOR.
   (4) Explotación de la info y SINFOR.
   (5) Negación de la infor y SINFOR.
   (6) Manejo de la info y SINFOR.

b. Cuando estas actividades son ejecutadas con efectividad: -suplementarán la habilidad humana de comando de batalla, - darán velocidad a la toma de decisiones, - minimizarán o eliminarán incertidumbres, - enfocarán la potencia combativa, - ayudarán a proteger la fuerza, - facilitarán el aprovechamiento de las posibilidades organizacionales, - enlazarán el AIM al IAG, y - mejorarán la conciencia situacional para las tropas y sus lideres.

c. Estas actividades se aplican tanto a la información como a los SINFOR (hardware, gente, organizaciones y procesos); y aunque estan listadas secuencialmente, ellas son concurrentes y parecidas en su aplicación. Ver figura 5, actividades de las OI.

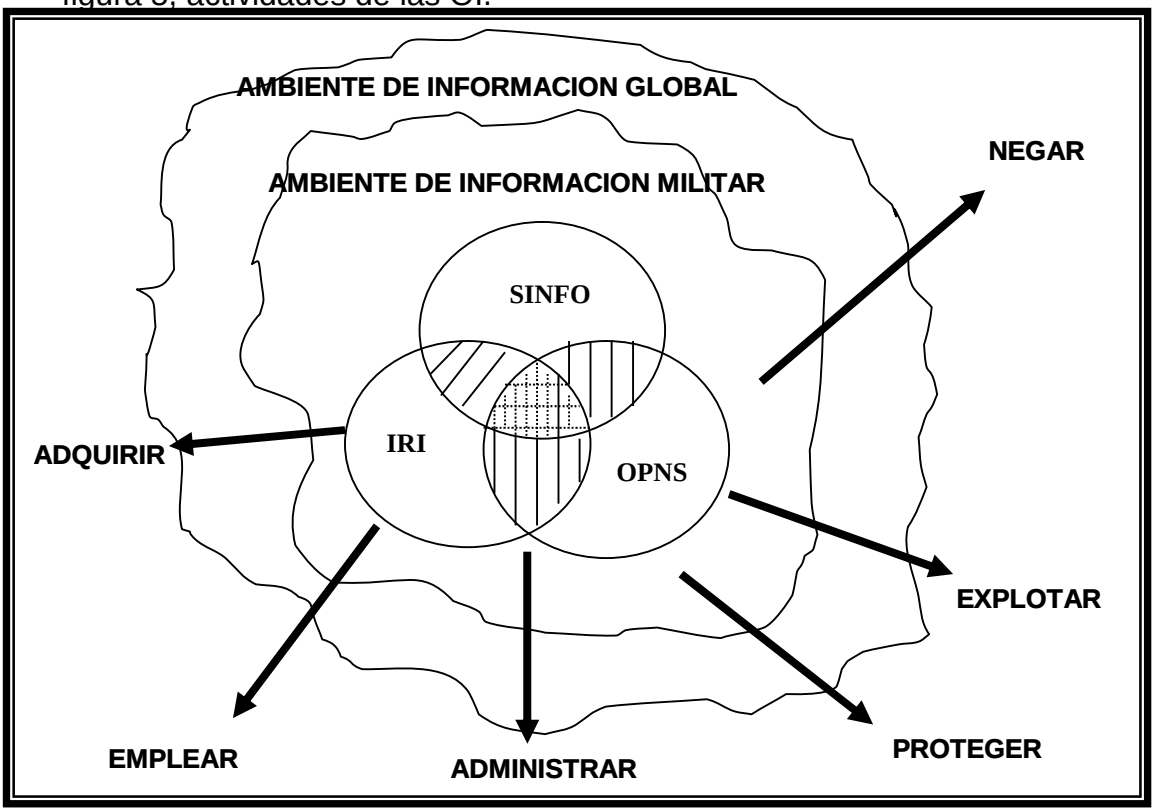

FIGURA 5: ACTIVIDADES DE LAS OPERACIONES DE INFORMACION

30. OBTENCION DE INFO Y SINFOR

a. Los Cmdtes deben considerar la naturaleza de la info que necesitan antes de distribuir los recursos para obtenerlos. Las preguntas iniciales que podría hacerse son:
   (1) ¿Cuál es la información que se necesita?
   (2) ¿Cuál es la naturaleza de esa información?
   (3) ¿Cómo puede obtenerse esa información?

b. Para la primera pregunta, normalmente la información necesaria incluye misión, enemigo, tropas, terreno y clima (CCMM), y tiempo disponible (METT-T); y la respuesta a las preguntas quién, qué, cuando, donde y por que. Para la segunda pregunta, la naturaleza de esa información incluye su precisión, oportunidad y la relevancia total a la situación en consonancia con las NICC. Para la tercera pregunta, la información puede obtenerse a través de las fuentes disponibles de info que incluyen personal, medios técnicos, sistemas de reunión de inteligencia, informes tácticos y la info e inteligencia difundida por los escalones superiores.

c. Considerando las fuentes de información disponibles y la naturaleza de esa info, los Cmdtes desarrollan planes técnicos y tácticos para obtener info crítica. La reunión de info sobre el adversario y sobre el ambiente es manejada a través del ciclo de reunión de IRI. Los Cmdtes determinan la info crítica para cada operación y pública aquellas necesidades a través de sus NICC. El Cmdte es el único quién decide que info será crítica basándose en su misión, en su experiencia y en la intención del Cmdte inmediato superior.

d. El EM puede recomendar NICC al Cmdte como:
   (1) Necesidades prioritarias de inteligencia (NPI), para determinar que desea o necesita el Cmdte conocer sobre el eno, su propósito y/o terreno (como veo al enemigo).
   (2) Necesidades de información de las fuerzas amigas (NIFA), para permitir al Cmdte determinar las posibilidades de combate (Cbte) de sus unidades o de las adyacentes amigas (como me veo a mi mismo)
   (3) Elementos esenciales de información amiga (EEIA), para permitir al Cmdte determinar como debe proteger la fuerza contra los sistemas de obtención de info enemigo (como puedo prevenirme que la fuerza ena me vea).

e. Las NICC normalmente están anotadas en el subparrafó 3.d (Instrucciones de coordinación) de una O/O o P/O. La info sobre las actividades amigas y su situación de operatividad son coordinadas tanto en el P/O o POV's de la unidad. La info también es obtenida empleando un ciclo de reunión de info más general desde otras fuentes e influencias en el AIM. Las necesidades de info del Cmdte no son satisfechas por una sola fuente, sino por:
   (1) Una combinación de sus propios sistemas electrónicos.
   (2) Actividades operacionales tales como reconocimiento y seguridad.
   (3) Actividades de inteligencia humana (INTHUMA)
   (4) Inteligencia estratégica o nacional.
   (5) Interface con medios noticiosos y policía local, nacional e internacional.

f. La info es perecedera y tiene cualidad temporal que a menudo es controlada por un juego de condiciones dinámicas o decisiones. Los eventos pueden hacer que una info llegue a ser irrelevante o no representativa como interpretar un marco altamente impreciso de la

realidad. La info más allá de cierta etapa disminuirá o desmerecerá la conciencia situacional del Cmdte. Los POV's, las NICC, los PP/OO y los planes de búsqueda, deben ser todos sensitivos a lo perecedero de la info; más aún, desde una perspectiva técnica los administradores de los SINFOR deben ser capaces de asegurar que la info y sistemas entregan oportunamente comunicaciones y entradas para la toma de decisiones.

31. EMPLEO DE LA INFO Y SINFOR

a. Un Cmdte debe ser hábil o capaz de ver su espacio de batalla en sus tres dimensiones (frente, profundidad y altura) para obtener info relevante y proveer una situación actual. El Cmdte expande su pensamiento incluyendo todos los SINFOR y organizaciones accesibles en el AIG. Una vez que los datos son obtenidos, analizados y, relacionados; la información será usada para actualizar y validar una conciencia situacional común, que proporcione la base para refinar, continuar o ajustar las decisiones, planes y operaciones:
   (1) La info es focalizada y empleada para emitir orientaciones, priorizar recursos y establecer necesidades.
   (2) Los EEMM refinan las orientaciones en los PP/OO y OO/OO, buscando integrar la info en todos los escalones y planes, empleando la disponible sin importar la fuente.

b. La info más oportuna, precisa o relevante, particularmente en operaciones de no-guerra; pueden venir de fuentes fuera de los canales de unidad o militares. Una unidad debe hacer empleo de los SINFOR orgánicos y no-orgánicos (dependencias del sector defensa, dependencias públicas y privadas, etc.), en este último caso coordinando con su elón superior debido a su complejidad. También se pueden emplear algunos servicios pasivos y abiertos, tales como la escucha o suscripción a medios de radiodifusión, revistas especializadas o técnicas, retrasmisiones de comunicaciones, pronósticos climáticos, etc; teniendo cuidado en la limitaciones legales, comerciales, económicas y políticas para su empleo.

c. Dependiendo de como las redes de comunicaciones dentro de una organización estén enlazadas o estructuradas, la información podrá fluir por múltiples conductos o vías. La interconexión de redes horizontalmente para SINFOR en los niveles más bajos posibles, proporcionarán un marco más profundo y multidimensional que los tradicionales informes de conductos o vías jerárquicas.

32. PROTECCION DE LA INFO Y SINFOR

a. Aunque la proliferación de la info y tecnología de la info puede ser una gran ventaja, será también un riesgo potencialmente significativo que debe ser considerado para cada operación. La protección de soldados y equipo, aunque no es nuevo, cobra una importancia creciente en el ambiente de abundante info hoy en día; por lo tanto la info amiga y sus SINFOR deben protegerse en todo el espacio de batalla. Operacionalmente, la protección de la info requiere "ver" las vulnerabilidades amigas a las perspectivas del ataque -C^2 enemigo. Los Cmdtes deben examinar la vulnerabilidad de sus soldados y sistemas a la explotación o ataque por un eno capaz de golpear el C^2 amigo sobre un frente amplio mediante el empleo de la GE, la destrucción, el engaño y la propaganda.

b. Para detener o retardar el funcionamiento de un sistema o arma, un adversario podría atacar la info o SINFOR que lo alimenta o sostiene. Por ejemplo, un adversario podría introducir un código de software malicioso a través de las redes de comunicaciones a los sistemas de dirección de tiro automático de artillería de campana o antiaérea, o también a los sistemas de alerta temprana, radares de vigilancia terrestre u otros medios que soportan a los SINFOR que emplean las armas y unidades. Las acciones que se toman para proteger la posibilidad de operar sin limitaciones en un AIM del espacio de batalla son consideradas parte de la G-C^2 (protección - C^2).

c. La info y los SINFOR deben protegerse en los niveles electrónicos, físicos y humanos, en ese orden, en relación a la amenaza potencial, sin impedir el funcionamiento o la operación total. Los programas de seguridad que identifican amenazas a los sistemas de C^4I también toman importancia creciente desde guarnición debido a lo "poroso" y abierto de la naturaleza del AIG que hace que la estructura de información del C^4I sea vulnerable al ataque o explotación en cualquier momento.

d. Como parte del planeamiento de las operaciones tanto en guarnición como en el espacio de batalla, el oficial de Telemática (G-6/S-6) deberá analizar la estructura de info de la unidad para priorizar que enlaces críticos, sistemas y datos deben protegerse. El G-6 debe tener en cuenta que todo no puede protegerse, por eso deberá coordinar con el oficial de operaciones (G-3/S-3) para realizar un análisis de la administración del riesgo que permita identificar info y SINFOR esenciales que deben mantenerse libres de dislocaciones o deformaciones de su contenido.

e. Los elementos de la infraestructura que deberán protegerse son datos, computadoras, sistemas de comunicaciones y facilidades o instalaciones que los soportan. Los planificadores debe integrar los elementos del AIG en los planes para asegurar que los Cmdtes consideren su impacto o potencial impacto en cualquier operación. La evaluación y los sistemas de análisis de vulnerabilidades deben proporcionar datos oportunos y precisos necesarios para identificar potenciales amenazas a los SINFOR amigos.

f. Un paso inicial básico en la protección total propuesta, es proteger sistemas de comunicaciones y computadoras contra la intromisión, trastornos y destrucción por acción enemiga. Sin embargo los Cmdtes también debe ser sensibles a los intentos enos de engaños y propaganda; este último recurso eno puede predisponerlo a él y a su EM a orientarse a una forma de acción (F/A) específica y luego explotar ese modo de pensar con una operación de engaño.

g. Las OI a menudo pueden tener lugar bajo condiciones degradas. Además un adversario o acciones accidentales o fenómenos naturales, pueden degradar o trastornar al equipo y servicios que provee. Debido a la fragilidad y complejidad de los SINFOR, un plan debería incluir procedimientos para operar sin toda la infraestructura de info.

33. EXPLOTACION DE LA INFO Y SINFOR

a. Todos los ambientes de información y sistema en tono a una operación, amigos y adversarios, militares y no-militares; ofrecen oportunidades para su explotación. Generalmente, la explotación de un SINFOR adversario es

hecho empleando comunicaciones o datos del SINFOR adversario sin su conocimiento.

b. Deberá preferirse una aproximación flexible para la explotación; esto es, que el nivel de explotación podría ir desde un simple monitoreo hasta corrupción o alteración de la base de datos, dependiendo de la situación y del objetivo deseado. La explotación no siempre significará un ataque o degradación directa sobre la habilidad de C^2 adversario.

c. La explotación envuelve:
   (1) La lectura de Telemática adversarias.
   (2) Interceptación de comunicaciones.
   (3) Análisis de Telemática.
   (4) Extracciones de base de datos.
   (5) Establecimiento del orden de batalla.
   (6) Tomar acción para negar, degradar o manipular aquellas posibilidades de la información.

d. La explotación depende de un entendimiento total del adversario y del AIG alrededor de una potencial zona de operaciones (Z/O). La obtención de info y el trabajo de inteligencia deben empezar desde época de paz, estableciendo el análisis de la Z/O (AZO) y como operan los potenciales adversarios. El conocimiento de la infraestructura de información adversaria es tan importante como el conocimiento de las estrategias y TTP's del adversario.

e. El conocimiento de la infraestructura de información del adversario permitirá evaluar a su personal, sus facilidades, sus sensores, sus procesadores y sus procesos de toma de decisión; buscando dar respuesta a la pregunta: "¿Que tanto depende o confía el adversario en el AIG para la información?". Esto a su turno afectará en como la unidad amiga interactua con el AIG, incluyendo los medios noticiosos, dependencias gubernamentales, ONG's y gobiernos extranjeros. La inteligencia ganada a través de la explotación apoyará al planeamiento y operaciones de la G-C^2, especialmente al engaño, a las operaciones sicológicas y a la destrucción física.

34. NEGACION DE LA INFO Y SINFOR

a. El aspecto ofensivo de las OI, ataq'-C^2, hace posible el objetivo de atacar a un adversario de manera simultánea en todos los niveles con una fuerza abrumadora. El ataq'-C^2 intenta impedir que un adversario ejercite el C^2 efectivo de sus fuerzas mediante la negación de info al adversario o influenciando, degradando o destruyendo la info y SINFO adversaria.

b. Las OI dan al Cmdte los medios para atacar a un adversario sobre toda la profundidad del espacio de batalla, más allá del alcance directo o indirecto de los sistemas de fuegos. El objetivo es degradar la confianza del adversario tanto en sus datos como en su habilidad para comandar y controlar sus operaciones. Atacando o confundiendo el sentido del campo de batalla, las fuerzas amigas ganan el dominio de la info y consecuentemente una ventaja relativa en la aplicación de la potencia combativa o controlar alguna situación en operaciones de no-guerra.

c. Las operaciones de negación de info generalmente demandan tiempo y ocurren sobre áreas relativamente grandes. Cegar o ensordecer un adversario requiere que muchos de sus sistemas principales de vigilancia y

reconocimiento sean influidos o enganchados; por eso, el ataque a los SINFOR adversarios normalmente son planeados como una serie de encuentros, enganches o combates que conducidos rápidamente y contra un objetivo específico, tal como la perturbación a un receptor de comunicaciones, radar de conducción de cohete (misil), etc; para destruir un nodo de C^2.

d. Para negar info a los adversarios que posean posibilidades de obtención espacial (sistemas satelitales) o vehículos aéreos no piloteados, los Cmdtes amigos deberán usar medios indirectos tales como el camuflaje o el engaño. En escalones división y menores, los Cmdtes pueden sufrir la falta de recursos para realizar todas las misiones del ataq'-C^2, particularmente aquellas que involucran engaño, operaciones sicológicas y GE; sin embargo, el valor de negar al adversario info permanecerá siendo importante y los Cmdtes de esos escalones deberán prepararse para contribuir a ese objetivo.

e. Los Cmdtes continuamente deben evaluar las posibilidades de explotar y negar, para adoptar un balance óptimo que alcance el mayor valor en el dominio sobre las OI enas. Las opciones de ataques múltiples en las OI resultarán del análisis y evaluación de objetivos potenciales. Generalmente, cuanto más temprano el ciclo de toma de decisión del adversario sea dislocado o perturbado más grande será el efecto que se pueda tener sobre sus posibilidades. Los Cmdtes operacionales deben sopesar la ventaja relativa que se puede ganar atacando los nodos de C^2 adversario contra la perdida potencial de inteligencia que se pudiera lograr de sus Telemática, radiaciones o emisiones y la necesidad para proteger las fuentes y métodos de inteligencia.

35. MANEJO DE LA INFO Y SINFOR

a. Para conducir operaciones dimensionalmente completas, la info y los SINFOR necesitarán cuidadosa coordinación y sincronización. Emitido el concepto inicial, el EM coordina e integra las necesidades de info y SINFOR para sincronizar el flujo de info crítico con el concepto operacional. El manejo de la info y SINFOR debe enfocarse sobre las necesidades operacionales que derivarán info desde los reconocimientos, contrareconocimientos, comunicaciones y operaciones de seguridad.

b. El manejo de la info incluye la administración del espectro electromagnético, decidir que fuentes y sistemas usar, asegurar un flujo de info confiable entre nodos y niveles (integración vertical y horizontal) y resolver las diferencias entre la info provenientes de múltiples fuentes.

c. Las necesidades operacionales guían la administración del espectro electromagnético, que servirá para el planeamiento y control de las funciones principales siguientes:
   (1) Comunicaciones.
   (2) Reunión o colección de inteligencia.
   (3) Perturbación electrónica.
   (4) Interferencia electromagnética.

d. Un efectivo manejo de la info y de los recursos permite que la info fluya horizontal y verticalmente a través de los sistemas operacionales del campo de batalla (SOC's) para posibilitar un efectivo planeamiento, preparación, toma de decisión y ejecución. La info también debería fluir

verticalmente entre escalones para facilitar el planeamiento paralelo o concurrente, eliminando la duplicación de esfuerzos y redundancia innecesaria, permitiendo a los sistemas tratar con lo sensitivo del tiempo y con info relevante. También reduce el nivel de ruido y Telemática de unidades en el espacio de batalla.

e. Las claves para comunicaciones y flujo de info efectivo son la conectividad total y la elasticidad. Las unidades pueden manejar la conectividad entre sus recursos orgánicos, pero la dificultad se presenta en el mantenimiento de una conectividad vertical y horizontal fuera de las unidades particularmente cuando se relacionan con fuerzas que emplean diferentes equipos de comunicaciones y SINFOR. La conectividad se cumple a través del establecimiento y mantenimiento de enlaces humanos y electrónicos, verticales y laterales fuera de la unidad, buscando compensar las menores capacidades tecnológicas de alguna fuerza con la preparación y despliegue de Oficiales de enlace con equipos compatibles de mejor tecnología.

f. La elasticidad es la habilidad de los SINFOR desde una perspectiva técnica y de administración, para proporcionar la necesaria conectividad y continuidad cuando los SINFOR son degradados. Adicionalmente, los líderes y planificadores en el ejército deben entender como la info militar y los sistemas se interconectan e interactuan con el AIG. Una sobrelasticidad en los sistemas comerciales, particularmente las redes de telecomunicaciones satélitales; pueden imponer restricciones o limitaciones a su empleo por fuerzas militares.

CAPITULO 3
GUERRA DE COMANDO Y CONTROL (G-C^2)

SECCION I. ROLES Y RELACIONES DE G-C^2

36. EVOLUCION DE LA G-C^2

a. Se ha mencionado en el párrafo 24, que para lograr la estrategia de las opns en profundidad, se ha desarrollado el concepto de las opns de guerra de cmdo y control; para integrar y sincronizar las posibilidades de las opns militares que hace pocos años eran planeadas y ejecutadas independientemente, conocidas como: seguridad de las opns (SEGOPE), guerra electrónica (GE), engaño militar, opns sicológicas y destrucción física. Estas opns constituyen hoy en día los cinco elementos fundamentales de la G-C^2.

b. La G-C^2 continua teniendo una tradicional orientación hacia el combate, tanto ofensiva como defensivamente, enfocándose sobre ideas de amenaza, conflicto y el campo de batalla, empleando varias técnicas y tecnologías para atacar o proteger un conjunto de objetivos de C^2 específicos que contribuya al dominio de la información sobre cualquier adversario o al control de una situación durante opns militares de no-guerra.

c. Aunque el concepto de G-C^2 fue desarrollado como un punto de referencia conjunto para las OI cuando se trabaja con EEMM conjuntos y otras fuerzas armadas en el marco de la guerra de información (G-I), en el ejército se debe interpretar que este nuevo paradigma debe ser más amplio y considerar la integración comprensiva de otras actividades de la info como fundamentales para todas las OI, surgiendo relaciones estrechas con las opns de asuntos civiles y opns de relaciones públicas.

d. A nivel conjunto, para que la G-C^2 sea efectiva necesitará que ésta se llegue a integrar totalmente al concepto de operación del cmdte y que este sincronizada con otras opns. La sincronización de estas acciones requerirá de un rápido y confiable apoyo de comunicaciones y de inteligencia. Un cmdte de una fza conjunta debería asegurarse que los objetivos de la G-C^2 sean parte de su orientación y prioridades de planeamiento.

e. A nivel ejército, la G-C^2 dirige su apoyo al objetivo de alcanzar el dominio de la información y ganar cualquier guerra, conflicto o subsiguientes en cualquier opn de no-guerra, rápida, decisivamente y con el mínimo de bajas. La G-C^2 incorpora el concepto de “espada y escudo” empleado en la GE; el escudo contra las acciones de atq‘- C^2 del adversario y la espada contra los sistemas de C^2 adversario. Esta combinación de aspectos ofensivos y defensivos en una capacidad integrada proporciona oportunidades expandidas para la sinergía en la guerra. La G-C^2 permite al ejército y cmdtes individualmente cumplir sus misiones con pocos riesgos, en marcos de tiempo más cortos y con menos recursos.

37. ROL DE LA G-C^2

a. La G-C^2 está definida como el empleo integrado de la SEGOPE, la GE, el engaño militar, las opns sicológicas y la destrucción física; apoyados mutuamente por la inteligencia; para negar info, influir, degradar o destruir las capacidades de C^2 adversaria; mientras protegemos las capacidades

b. de C^2 amigo contra tales acciones. La G-C^2 se aplica a través del contínuo operacional y en todos los niveles del conflicto.
c. La G-C^2 se aplica también a todas las fases de las opns, incluyendo aquellas que se realizan antes, durante y después de las hostilidades en curso. Aún en opns de no-guerra, la G-C^2 ofrece al cmdte militar medios para cumplir la misión asignada mientras detiene la guerra y/o promueve la paz.
d. El aspecto ofensivo de la G-C^2 puede hacer lento el ritmo operacional adversario, desarticular sus planes y habilidad para enfocar su potencia combativa; e influir su apreciación de la situación. El aspecto defensivo de la G-C^2 minimiza las vulnerabilidades del sistema de C^2 amigo y la interferencia mutua.

38. RELACIONES DE LA G-C^2

a. La G-C^2, como parte de las OI propiamente dicha tiene estrecha relación con las opns civiles - militares o más comúnmente conocida como opns de asuntos civiles y con las opns de relaciones públicas. Estas tres opns están mutuamente en roles de apoyo tal como se muestra en el cuadro de doble entrada de la figura 6, redes de apoyo mutuo de G-C^2, AC y RP.
b. Aunque las actividades de AC y RP no son tratados en este manual de manera extensiva, sus roles en un mundo tan globalizado como el de hoy, han hecho que incremente su importancia para el apoyo a un conflicto moderno. Los elementos y disciplinas de la G-C^2 no podrán desarrollarse apropiada y eficientemente si es que no han sido coordinadas e integradas sus acciones con las opns de AC y de RP; con lo cual, las OI serán consistentes con la misión de la fuerza.

	G-C^2	**ASUNTOS CIVILES (AC)**	**RELACIONES PUBLICAS (RP)**
LA G-C^2 PUEDE APOYAR:		**Influyendo/informando a población de actividades y apy de AC.** **Neutralizando desinformacion y propaganda hostil dirigida contra autoridades civiles.** **Controlando el espectro electro-magnético para propósitos de comunicaciones legitimas.** **Proporcionando miles de productos de info para apoyar los esfuerzos de AC.**	**Conduciendo contra-propaganda y protegiendo contra rumor o malinformación.** **Desarrollando EEIA para impedir una revelación publica inavertida.** **Sincromizar las opns sicologicas y la SEGOPE con la estrategia de RP.**
LOS AC PUEDEN APOYAR:	**Proporcionando INFO para apoyar al marco de la infraestructura de la INFO** **Sincronizando los medios de Com. y mensajes con las opns/sicolog.** **Coordinando el juego de objetivos de C^2 con la celda objetivo.** **Estableciendo y manteniendo enlace o dialogo con personal local/nativo, ONG's, OPV's.**		**Proporcionado info de las actividades de AC para apoyar la estrategia de RP.** **Sincronizando la info, medios de com. y mensajes.** **Identificando, coordinando e integrando los medios de info pública de la Z/O**
LAS RP PUEDE APOYAR:	**Desarrollando productos de info para proteger a soldados contra efectos de desinformación o malinformación.** **Coordinando con opns/sicolog para asegurar consistencia de**	**Produciendo info precisa, oportuna y balanceada para el público.** **Coordinando con especialistas de AC para verificar hechos y validar info.**	

	mensajes y mantenimiento de opns/sicolog.		

Figura 6: ROLES DE APOYO MUTUO DE G-C², AC Y RP

SECCIÓN II. ELEMENTOS DE LA G-C²

39. CONSTRUCCION DE LOS ELEMENTOS DE LA G-C²

a. Los cimientos para una G-C² son sistemas de información (SINFOR) robustos y redundantes de comando, control, comunicaciones y computación (C⁴), asociados con información relevante, perfecta y fluyendo de nivel nacional al táctico, con apoyo de la inteligencia.

b. Sobre estos cimientos descansan los bloques del edificio de la G-C², conocidos como elementos, que incluye:
   (1) Seguridad de las opns (SEGOPE)
   (2) Engaño militar
   (3) Opns sicológicas (opns/sicolog)
   (4) Guerra Electrónica
   (5) Destrucción física

c. Estos bloques del edificio contribuyen a la protección de la fuerza y cumplimiento de la misión de varias maneras, dependiendo de la situación. Esta dependencia guía la conformación u ordenamiento de los bloques, cambiando constantemente su patrón tal como se muestra en la figura 7, construcción de la G-C². El empleo integrado de estos cinco bloques o elementos conduce a la sinergia sobre el campo de batalla y resulta en una ejecución más efectiva de las tareas del atq' – C² y/o protección – C². El cmdte dirige este proceso de G-C² para lograr agilidad enfocando su ataque sobre la habilidad adversaria para comandar y controlar sus fuerzas, mientras que simultáneamente protege el C² amigo.

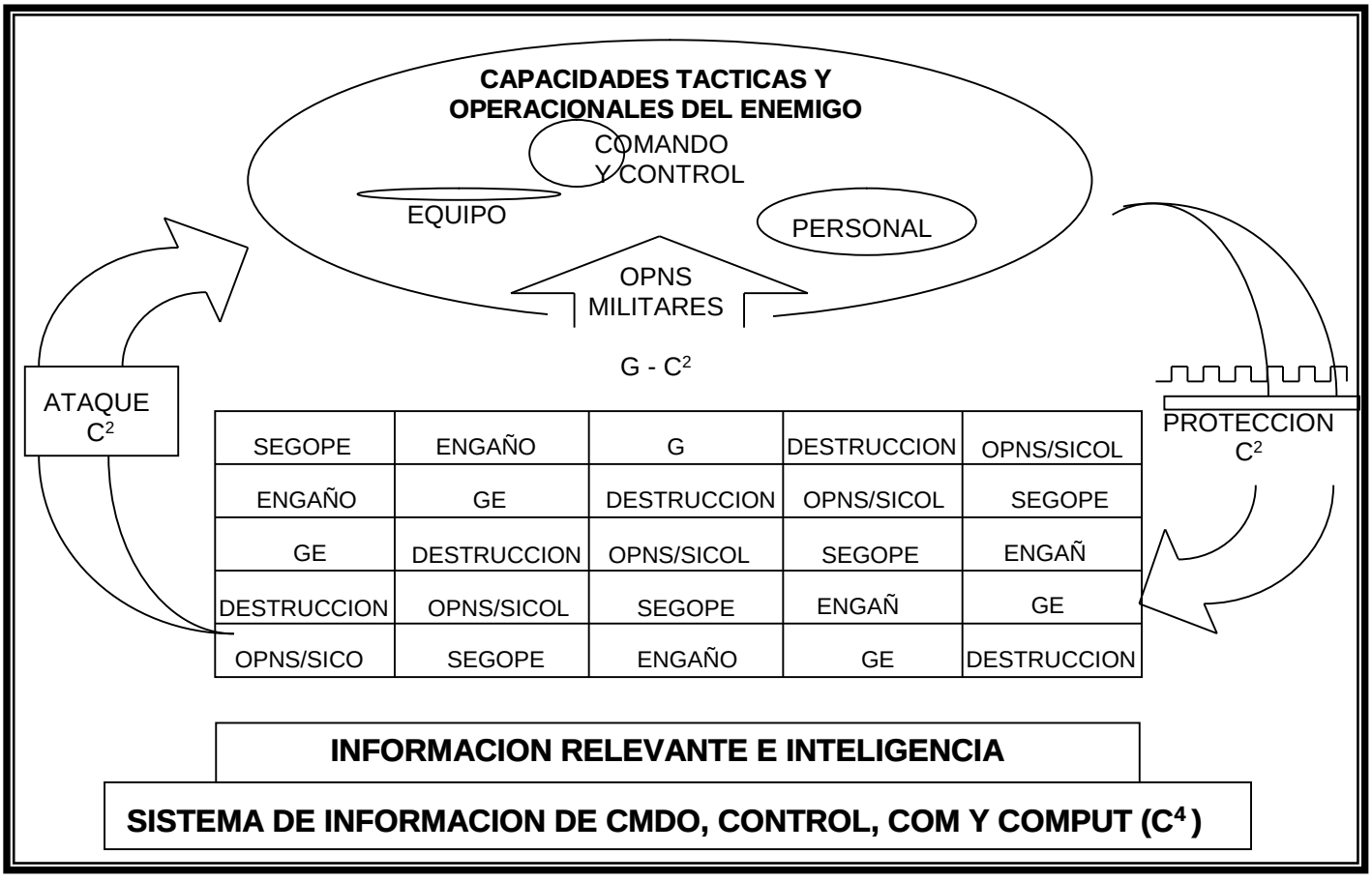

Figura 7: CONSTRUCCION DE LA G-C2

40. SEGURIDAD DE LAS OPERACIONES (SEGOPE)

a. La SEGOPE es la clave para la negación. Ella da al cmdte la capacidad de identificar aquellas acciones que pueden ser observadas por los sistemas de inteligencia adversaria y puede proporcionar una conciencia de los potenciales indicadores amigos que los sistemas de inteligencia adversaria podría obtener. Tal conciencia podría ser interpretada o piezada junta para derivar información crítica sin interesar el dispositivo, intención y/o formas de acción amiga que debe protegerse. El objetivo de la SEGOPE es identificar, seleccionar y ejecutar medidas que eliminen o reduzcan, a un nivel aceptable, indicaciones y otras fuentes de información que podrían ser explotadas por un adversario.

b. El planeamiento de la SEGOPE está severamente retada por la nueva familia de capacidades comerciales globales, que incluyen sistemas de imágenes geomáticos, sistemas de posicionamiento global y sistemas de comunicaciones personales y celulares; que ofrecen a los potenciales adversarios acceso a un nivel de información sin precedentes contra las fuerzas amigas. Por otro lado, la presencia inevitable de los medios noticiosos durante las opns militares complica la SEGOPE, ya que estos tienen la capacidad para trasmitir o difundir información en tiempo real a todo el mundo, que podría ser una fuente de información lucrativa para un adversario. Los planificadores de la SEGOPE deben trabajar estrechamente con personal de relaciones públicas, para el desarrollo de elementos esenciales de información amiga (EEIA) que impidan la revelación pública inadvertida de información crítica o sensitiva.

c. Muchas medidas diferentes impactan sobre la SEGOPE, incluyendo la contrainteligencia, la seguridad de la información, la seguridad de la trasmisión (SEG/TRASM), la seguridad de comunicaciones (SEG/COM) y la seguridad electrónica. Conforme el ejército vaya digitalizando todos los SINFOR, la seguridad de la información tomará mayor importancia.

d. Mayor información sobre la SEGOPE puede encontrarse en el manual de Seguridad de Comunicaciones en el capítulo 1 (Edición 1998).

41. ENGAÑO MILITAR

a. El engaño militar es el medio principal para influir en las decisiones del comandante adversario, mediante la distorsión, cubrimiento y/o falsificación de las intenciones, situación, dispositivo, capacidades, formas de acción y fuerza de nuestras tropas.

b. El objetivo del engaño es causar que el cmdte militar opuesto actúe en una forma que sirva a los objetivos de los cmdtes amigos. Mayor información sobre las opns de engaño pueden encontrarse en los manuales respectivos.

42. OPERACIONES SICOLOGICAS (OPNS/SICOLOG)

a. Las opns/sicolog están basadas en la proyección de mensajes verdaderos y creíbles, siendo una herramienta esencial en las opns de G-C^2 y cuando se combinan con el engaño militar y la SEGOPE se constituyen en un poderoso multiplicador de la fza. Las opns/sicolog pueden: hacer proliferar mensajes discretos hacia los colectores de C^4 adversario; mejorar las

demostraciones de potencia combativa conjunta con llamados a la rendición; y magnificar la imagen de superioridad tecnológica o de experiencia y entrenamiento de combate.

b. Los elementos de las opns/sicolog deben trabajar estrechamente con los otros elementos de la G-C^2 y estrategas de relaciones públicas para maximizar la ventaja de las operaciones de información.

c. El principal objetivo de las opns/sicolog dentro de la protección de C^2 es minimizar los efectos de la campaña de desinformación y propaganda de un adversario hostil contra nuestras fuerzas. Desacreditando dicha propaganda y malinformación contra las opns amigas será la principal manera para mantener una opinión pública favorable a nuestras opns.

d. Mayor información sobre las opns/sicolog pueden encontrarse en los manuales respectivos.

43. GUERRA ELECTRONICA (GE)

a. Actualmente las subdivisiones de la GE se denominan:
   (1) Ataque electrónico (antes contramedidas electrónicas: COME).
   (2) Protección electrónica (antes contra-contramedidas electrónicas: COCOME)
   (3) Apoyo de guerra electrónica (antes medidas de apoyo de GE: MAGE).

b. Todo lo referente a la GE está ampliamente desarrollado en los manuales de doctrina general de guerra electrónica y empleo táctico de la guerra electrónica (ediciones 1998). Sin embargo, cabe mencionar que las posibilidades del ataque electrónico se han incrementado hoy en día, ya que pueden atacar a un adversario prácticamente en cualquier lugar desde donde intente usar equipos con energía electromagnética. Por otro lado, la protección electrónica ha cobrado una mayor importancia en cuanto a sus aspectos activos para llegar a ser parte de las opns de supervivencia, en vista que muchos sistemas de armas vienen empleando casi el 100% componentes electrónicos y al espectro radioeléctrico. Finalmente, el apoyo de guerra electrónica ha pasado a formar parte del concepto de información de combate que permita capitalizar con oportunidad y de manera inmediata la detección de sistemas sensores y de guiado/conducción radioeléctrica de Telemática o misiles.

44. DESTRUCCION FISICA

La destrucción de un C^2 hostil significa que las capacidades o posibilidades de C^2 adversaria serán degradadas por un período de tiempo, o si fuera necesario, inutilizadas permanentemente. La destrucción física sólo será empleada después de una total evaluación comparativa (desde las perspectivas estratégicas hasta tácticas) del equilibrio entre preservar objetivo versus su destrucción.

45. RELACIONES POTENCIALES Y CONFLICTOS ENTRE LOS ELEMENTOS DE LA G-C^2

Los elementos de G-C^2 encierran una serie de relaciones cuando interactuan entre ellas, las mismas que pueden ser de apoyo mutuo o de potenciales conflictos. Será de responsabilidad del cmdte y de los planificadores de cada

uno de estos elementos de reforzar el apoyo y minimizar los potenciales conflictos. Las figuras 8 y 9 "(de la página siguiente)", donde se muestran un cuadro de doble entrada en cada una de ellas, ilustran algunas de las relaciones de apoyo mutuo y potenciales conflictos, respectivamente.

SECCIÓN III. DISCIPLINAS DE G-C^2

46. ATAQUE DE COMANDO Y CONTROL (Atq´- C^2)

a. Definición.- El Atq´- C^2 está definido como la ejecución sincronizada de acciones que se toman para cumplir los objetivos establecidos para prevenir el C^2 efectivo de las fuerzas adversarias mediante la negación, influencia o degración de la información, o mediante la destrucción del sistema de C^2 adversario.

b. Principios:
   (1) Planear basándose en la misión de la unidad, en la intención del cmdte y en su concepto de operaciones.
   (2) Sincronizar con el plan del cmdte y apoyar al mismo.
   (3) Tomar y mantener la iniciativa mediante la degradación de los SINFOR adversarios y forzándolo a ser reactivo (Reactivo significa que el atq´- C^2 hace lento el ritmo adversario, disloca y perturba los ciclos de decisión y planeamiento adversario, trastorna la habilidad del cmdte adversario para generar potencia combativa y degrada los medios del cmdte adversario para ejecutar sus órdenes tipo-misión y controlar las opns de sus unidades subordinadas).

c. Efectos.- En términos generales, el atq´- C^2 tiene cuatro (04) efectos que se enfocan sobre la infraestructura de C^2 y flujo de info del adversario para producir sobre él que su proceso de toma de decisión sea más lento y de menor calidad que el nuestro:
   (1) Primero, al adversario se le niega información a través de: la perturbación o niebla de su observación; degradación de su orientación, formulación de su decisión y sistemas de reunión de info. Esta última pueda ser degradada mediante la destrucción de los medios de búsqueda, influenciando sobre la info que obtenga el adversario o provocando que éste no reúna toda la info que necesitaria para armar un marco general.
   (2) Segundo, al cmdte adversario se le influencia mediante la manipulación de su percepción y causando desorientación de su ciclo de decisión.
   (3) Tercero, a las OI adversarias se las degrada mediante la dislocación y trastorno de selectivos sistemas de C^4I.
   (4) Cuarto, las posibilidades de info adversarias pueden ser neutralizadas o destruidas por la destrucción física de los nodos y enlaces de info (Ver párrafo 5 del Manual de Seg de Com Ed 1998).

47. PROTECCION DE COMANDO Y CONTROL (Protección – C^2)

a. Definición.- La protección – C^2 está definida como el mantenimiento de un C^2 efectivo de nuestras propias fuerzas convirtiéndolo en ventaja amiga o neutralizando los esfuerzos adversarios por negarnos info, o para destruir, degradar o influir el sistema de C^2 amigo.

b. Principios.-

(1) La protección–C^2 puede ser ofensivo o defensivo. En el primer caso usa los cinco (05) elementos de la G-C^2 para reducir la habilidad adversaria para conducir su atq'-C^2, y el segundo caso reduce las vulnerabilidades de C^2 amigas al atq´-C^2 adversario mediante el empleo de una protección adecuada física, electrónica y de intelig.

(2) Este doble aspecto de la protección de C^2 hace que para entender su proceso, el cmdte deba preguntarse como el adversario podría emplear sus opns de destrucción, de GE, de engaño, de SEGOPE y Opns/Sicolog para trastornar nuestros sistemas de C^2 y proceso de toma de decisiones. Haciendo un juego de guerra con las formas de acción de atq´- C^2 adversario, el cmdte puede desarrollar una opn de protección comprensiva sincronizada con el esfuerzo principal y con el propio ataque – C^2.

(3) De acuerdo a lo establecido en los sub-párrafos precedentes, el cmdte guiará sus opns de protección – C^2 con los principios sgtes:

(a) Ganar la superioridad de C^2.- Esto incluye funciones tales como procesamiento de info amigo continuo, desarrollo de formas de acción precisas, toma de decisiones válidas y comunicaciones eficientes hacia y desde los subordinados.

(b) Permanecer dentro del ciclo de decisión adversario.- Esto es hecho mediante la negación, influencia, degradación y/o destrucción de los sistemas de C^2 adversario; así como de su personal y equipos (Ver Manual de Empleo Táctico de GE párrafos 3 al 6 Ed 1998).

(c) Reducir la habilidad adversaria para conducir su atq´- C^2.

(d) Reducir las vulnerabilidades de C^2 amigas empleando medidas de protección de C^2, como por ejemplo contrarrestar los efectos de la propaganda o malinformación adversaria, mediante las tareas críticas de los recursos de GE para proteger el C^3 amigo (Ver párrafo 6 del manual de Seg de Com Ed 1998).

(e) Reducir la interferencia mutua de nuestros sistemas de C^3 mediante la administración del espectro electromagnético.

c. Efectos.-

(1) Los efectos de la protección de C^2 reflejan aquellos del atq´ - C^2; ya que podemos negar info que el adversario necesita para tomar una acción efectiva, podemos influir sobre el adversario para que no tome ninguna acción, tome una acción incorrecta o tome una acción en un momento no oportuno. También podemos degradar y destruir sus capacidades para realizar su atq´- C^2 contra fuerzas amigas.

(2) Las opns/sicolog y las opns de RP apoyan a la protección de C^2. La primera puede abrir una brecha ente el liderazgo adversario y su población para debilitar la confianza y efectividad del liderazgo adversario; las opns de RP a través de un "programa de info interno del cmdte" pueden beneficiar poderosamente para contrarestar la propaganda adversaria contra el país y fuerzas nacionales desplegadas, así como trabajando coordinadamente con personal especialista de inteligencia y de opns/sicolog se puede proteger a las tropas preparando productos que pueda emplear el cmdte contra los efectos de la desinformación y malinformación adversaria.

CAPITULO 4
INFORMACION RELEVANTE E INTELIGENCIA (IRI)

SECCION I. FUNDAMENTOS DOCTRINARIOS DE INFO RELEVANTE

48. ROL DE LA INFO RELEVANTE

a. Definición.- La info relevante está definida como aquella extraída del ambiente de info militar (AIM) que significativamente impacte, contribuya o este relacionada a la ejecución de la misión operacional en curso (que se está desarrollando).

b. Relación de la info relevante con el AIM.- La info relevante tiene una relación directa con el AIM en dos maneras:
   (1) Primero, el acto de buscar, reunir, procesar y/o difundir info relevante sirve como el criterio principal que un Cmdte aplica, para incluir un individuo, una organización o un sistema como parte de un AIM.
   (2) Segundo, el AIM es el producto o el medio de donde se extrae info relevante o es usado por los mismos protagonistas o actores que sirven como base de las OI.

c. Importancia actual del concepto de información relevante
   (1) En el pasado la tendencia ha sido aproximar la orientación del esfuerzo de búsqueda, la reunión de info y su empleo operacional desde una perspectiva especializada. Por ejemplo, los diferentes elementos de los sistemas operacionales del campo de batalla (SOC's) han reunido y empleado su necesaria info para apoyar sus funciones particulares, tales como:
      (a) La inteligencia enfocándose sobre la info del adversario y países extranjeros de interés.
      (b) Los que maniobran enfocándose sobre el sostenimiento de las condiciones y necesidades de las fuerzas amigas.
      (c) Los logísticos enfocándose sobre le sostenimiento de las condiciones y necesidades de las fuerzas amigas.
      (d) Las comunicaciones y la GE enfocándose en dominar o alcanzar la superioridad del espectro electromagnético.
      (e) Los AC y las RP enfocándose en el interface entre sectores militares y no-militares.
   (2) Sólo una pequeña cantidad de tales informaciones era compartida, y normalmente en niveles relativamente altos dentro de una organización jerárquica militar. La info fluía de arriba hacia abajo como un ducto con rutas que tendían a hacer lento la posibilidad de compartir la info a través de los límites organizacionales. Aún hoy en día, los esfuerzos por enfocarse en la integración y sincronización de la info son escasos o casi nulos; a pesar que se vienen desarrollando una serie de base de datos especializados para necesidades particulares sobre el campo de batalla.
   (3) El primer paso para la integración y sincronización de los esfuerzos de búsqueda, reunión, procesamiento y difusión de info relevante, será la creación y desarrollo de un sistema de C^4I, que nos permitirá enfrentar los cambios en la era de la info, para alcanzar nuevos niveles de

eficiencia y efectividad en el empleo de la info. El siguiente paso, será enfocar los esfuerzos para apalancar o balancear la potencial contribución operacional de la info, reuniéndola y compartiéndola eficientemente a través de todos los elementos de los SOC's.

49. CRITERIOS DE EVALUACION DE LA INFO RELEVANTE

a. Debido a que las fuentes de info son imperfectas y susceptibles de distorsión y engaño, los Cmdtes y planificadores deben evaluar cuidadosamente la calidad de la información antes de su empleo. El ME 38-5 en sus párrafos 73 al 77 (Ed. 1983), establece unos criterios para evaluar y valorizar la info como base para su subsecuente interpretación. Este manual propone otros criterios que pueden emplearse conjuntamente con los anteriores o de acuerdo a la situación y experiencia del Cmdte y planificadores:
   (1) Exactitud.- La info expresa la situación verdadera.
   (2) Relevancia.- La info puede aplicarse a la misión, tareas o situación.
   (3) Oportunidad.- La info que está disponible en el momento de tomar decisiones.
   (4) Utilidad.- La info que está mostrada o formateada de manera que sea fácilmente entendible y común para todos.
   (5) Completa.- La info que es necesaria para que se tome una decisión.
   (6) Precisa.- La info que está presentada a un nivel de detalle requerido.

b. Como una primera prioridad, la info debería ser exacta y relevante; luego debería ser oportuna y útil; y finalmente debería ser tan completa y tan precisa como sea posible. Cuando se evalúe se recomienda seguir o tener en cuenta las relaciones siguientes:
   - Info incompleta o imprecisa es mejor que ninguna info.
   - Info inoportuna o inútil es la misma que ninguna info.
   - Info inexacta o irrelevante es peor que ninguna info.

50. LA INFO RELEVANTE DENTRO DEL CICLO DE DECISION DEL CMDTE

a. Los Cmdtes deben tener info para comandar, ya que ella será el medio que le permitirá funcionar a su proceso o ciclo de decisión y ejecución. La info dará dirección a las acciones para la fuerza, proporcionándole formas de acción para protegerla y ayudarla a cumplir su misión operacional.

b. La info relevante extraída del AIM apoya la creación de la conciencia situacional que contribuye directamente a un C^2 efectivo durante las cuatro (04) fases del ciclo de toma de decisiones del Cmdte (ver párrafos 4 y 11 del manual de Empleo Táctico de GE, Ed. 1998). El C^2 en un ambiente de conciencia situacional ayuda al Cmdte a asegurar la unidad de esfuerzo orientado hacia el cumplimiento de la misión. Finalmente el C^2, dependerá que la persona correcta tenga la info correcta en el momento correcto.

c. Como se menciona en el manual de Empleo Táctico de Guerra Electrónica, el ciclo o proceso de toma de decisiones del Cmdte consta de cuatro pasos o fases, dentro de las cuales la información relevante toma lugar. A continuación se hará un breve descripción de cada paso y su relación con la información relevante:

(1) Paso 1: Análisis de la situación.- Lo primero que debe tenerse presente es que el Cmdte es el elemento central de todo el proceso de C^2; de acuerdo a esto él se esfuerza por entender su situación actual y ambiente mediante la obtención de info relevante sobre su espacio de batalla y el estado de las fuerzas importantes (amigas y adversarias), empleando todas las fuentes disponibles, incluyendo personal de observación, sensores remotos, SINFOR e informes de sus subordinados, que lo lleven a visualizar el campo de batalla.

(2) Paso 2: Planeamiento.- Después de recibir la misión, el Cmdte combina su entendimiento del ambiente actual, visualiza un futuro estado final deseado y desarrolla un concepto inicial de como ejecutar la misión.

(3) Paso 3: Emisión de ordenes.- Basado en su entendimiento de la situación y su intención, el Cmdte emite su concepto de operaciones y dirige el planeamiento para desarrollar y refinar una forma de acción viable, aprobada por él, que le permitirá cumplir su misión. Esto se materializa con la preparación, aprobación y emisión de ordenes que pondrán a la operación en movimiento; es decir, que se dará inicio a la fase o ciclo de ejecución.

(4) Paso 4: Supervisión.- Durante la fase de ejecución, el Cmdte monitorea la operación y estima sus resultados. Esto trae a él todo el ciclo para obtener info nueva o adicional desde la cual empezará nuevamente el ciclo, que continuamente afectará la habilidad del Cmdte para obtener info, visualizar, planear, decidir y ejecutar.

d. Desde que el ciclo de toma de decisiones y de ejecución es un proceso continuo, todas las partes del mismo son activadas en cada escalón de comando; es decir, los Cmdtes reúnen info, desarrollan conciencia situacional y planean operaciones futuras al mismo tiempo que conducen operaciones en curso. Pero para mantener un ciclo de decisión y ejecución rápido, consecuentemente un ritmo de operaciones rápido, se requiere que el Cmdte de la fuerza y sus Cmdtes subordinados tengan un cuadro común y exacto del espacio de batalla, desde el cual la unidad ganará mayor conciencia situacional con la cual ejercer la iniciativa durante el combate u otras situaciones.

e. El Cmdte opera dentro del AIG ajustando su AIM como sea necesario para mejorar su conciencia situacional. Más aún, el Cmdte emplea varios medios en el AIM para asegurar que todos los elementos de su fuerza tengan una conciencia situacional común, completa y relevante. Esto demanda un SINFOR sofisticado que mejore la habilidad del Cmdte para conformar, manejar y mover la info entre las organizaciones.

SECCION II. FUNDAMENTOS DOCTRINARIOS DE LA INTELIGENCIA

51. ASPECTOS CONCEPTUALES SOBRE LA INTELIGENCIA

a. Definición de Inteligencia.- Inteligencia es el producto resultante de la reunión, procesamiento, integración, análisis, evaluación e interpretación de la info disponible concerniente a países de interés o áreas. También es, la info y el conocimiento sobre un adversario obtenida a través de la observación, investigación, análisis o entendimiento.

b. La inteligencia también es un subelemento crítico de la información relevante que se concentra principalmente sobre ambientes extranjeros y el adversario. Contra un adversario, la inteligencia es vital para desarrollar y ejecutar operaciones efectivas de G-C^2 que degraden y distorsionen los procesos de toma de decisiones del enemigo, al mismo tiempo que protegemos el C^2 amigo.

c. En apoyo a las operaciones amigas, la inteligencia ayuda a producir un marco del espacio de batalla común, actual y relevante, que reduzca las incertidumbres y falencias en el proceso de toma de decisión del Cmdte. Igualmente, la inteligencia que apoya a la G-I, ejecutada en los niveles estratégico y nacional; debe ser apalancada para apoyar a la G-C^2 y a las OI conducidas en los niveles operacional y táctico. Este esfuerzo requiere un proceso de búsqueda-reunión de inteligencia casi perfecto, apoyado en una arquitectura de comunicaciones que permita fluir y proveer los productos de inteligencia en tiempo-real orientado a las necesidades de info críticas del Cmdte (NICC).

52. ROL DE LA INTELIGENCIA

a. La inteligencia proporciona al Cmdte un entendimiento exacto de la situación de la amenaza y su relación con las operaciones actuales y futuras. El personal de inteligencia obtiene, usa, maneja y explota info para producir tal entendimiento.

b. Para que una conciencia situacional común sea exacta y actual, el esfuerzo de inteligencia será un proceso continuo de búsqueda-reunión incluyendo a todas las fuentes posibles, desde las operaciones cubiertas del nivel nacional hasta las fuentes abiertas locales, tales como los medios noticiosos, contactos comerciales, académicos y personas del lugar.

c. En operaciones de no-combate, la inteligencia humana, las fuentes abiertas y otras dependencias públicas y/o privadas; pueden proporcionar info oportuna para mejorar el esfuerzo tradicional de una unidad enfocado a la búsqueda-reunión de inteligencia de combate o batalla. La inteligencia apoyará a la G-C^2 enfocándose en sus dos disciplinas (ataq'-C^2 y protección-C^2)

53. FUNCIONES O ACTIVIDADES QUE APOYA LA INTELIGENCIA

a. El principal propósito de la inteligencia es posibilitar decisiones operacionales bien informadas, basadas, en un entendimiento exacto de la situación. La esencia de la inteligencia es reunir, analizar, proteger y presentar info que necesita el Comandante; que lo ayude a reducir sus incertidumbres mediante la eliminación de info que no es relevante para su proceso de toma de decisiones. De acuerdo a lo expuesto, la inteligencia apoya principalmente a las funciones o actividades siguientes:
   (1) Evaluación de las vulnerabilidades amigas.
   (2) Entendimiento del adversario.
   (3) Empleo de la preparación de inteligencia del campo de batalla (PIC)
   (4) Evaluación de daños de batalla.

b. Evaluación de las vulnerabilidades amigas
   (1) El primer paso crítico en la protección de las posibilidades de las OI será identificar amenazas potenciales y específicas. Las amenazas potenciales van desde acciones adversarias directas abiertas y

cubiertas, pasando por individuos y organizaciones buscando explotar los SINFOR militares, hasta fenómenos naturales; incluyendo una nueva familia de sistemas comerciales globales de geomática, imágenes, telefonía de PCS (terrestre y satelital) y de posicionamiento (GPS); que conjuntamente o separadas proveen a los potenciales adversarios con info en tiempo casi-real sobre fuerzas y movimientos.

(2) La naturaleza fluida y porosa del AIM hace difícil proteger los SINFOR de posibles ataques; de ahí que la inteligencia provee al Cmdte con la info necesaria para conducir evaluación de riesgos y desarrollar opciones de administración del riesgo para proteger componentes y capacidades vitales de C^2. La evaluación del riesgo está basada en la identificación de factores tales como capacidades específicas de la amenaza, sus capacidades técnicas, su doctrina y su rendimiento anterior; sin embargo, la evaluación del riesgo no es un documento final sino un proceso continuo que constantemente será actualizado para reflejar cambios en el ambiente operativo, tecnológico y sistemas de adquisición de la amenaza (mayor info sobre procesos de evaluación de riesgos pueden encontrarse en los manuales de seguridad de Com. Ed. 1998, operaciones y organización de EM de Com. Ed. 1999).

(3) Debido a que dentro del concepto de G-C^2 se presentan a los potenciales adversarios oportunidades para golpear a la infraestructura de las fuerzas, donde sea que estas se localicen, los Cmdtes y sus EEMM deben estar conscientes de las amenazas a sus SINFOR desde su estación base en territorio o área propia hasta la desplegada en zonas adelantadas o territorio no propio.

c. Entendimiento del adversario

(1) La efectividad del ataq'-C^2 está basada en un entendimiento total de un adversario, su sistema de C^2 y su proceso de toma de decisiones. Cuanto más profundo sea el entendimiento, asociado a técnicas y herramientas para tomar ventaja de tal conocimiento; más efectiva será la explotación de un adversario potencial.

(2) En todos los niveles de la guerra, la inteligencia es una herramienta operacional que identifica, evalúa y explota la info y sistemas de C^2 enemigo. Los datos que se requieren son: que info busca y reúne el adversario, porque medios, que confiabilidad asigna a sus fuentes y como evalúa su data.

(3) El personal de inteligencia debe ser capaz de describir los procesos de toma de decisiones del eno y como los direcciona para enviarlas a sus subordinados. También se requiere inteligencia de detalle sobre los ambientes social y cultural y perfiles sicológicos de los líderes claves y personas que toman decisiones en el adversario. Como ellos interactúan y se perciben uno a otro, son aspectos importantes de la info necesaria para desarrollar operaciones/sicológicas efectivas y operaciones de engaño. Finalmente, el sabor como los subordinados del Cmdte adversario ejecutan las decisiones, completará el cuadro del entendimiento total.

(4) El tener un entendimiento detallado de como el adversario usa la info, será necesario para determinar donde y como influenciar sus acciones

de manera efectiva. La figura 09, da una idea general de como el dominio de la información permite entender al adversario.

d. Empleo de la PIC

(1) Gran parte de lo referente a la preparación de inteligencia del campo de batalla es tratado en el manual de empleo táctico de GE (Ed. 1998); pero en el contexto de este manual, la PIC es un proceso continuo empleado para desarrollar un conocimiento detallado de los sistemas de información adversaria, con acciones traslapadas y simultáneas que producen la actualización de la situación sobre una base continua y proveer opciones al Cmdte.

(2) Está forma de PIC de la información será la base para el planeamiento de las OI y para el desarrollo de formas de acción de G-C^2 y para la determinación de objetivos del mismo, que incluyen: los que toman decisiones, el proceso de decisión y los nodos de C^2. Las otras consideraciones en las OI en la PIC de la info son, que deben basarse en la maniobra y en el conocimiento, estar orientado al equipo, a la fuerza y a la decisión, "buscando que el adversario no piense ni se comunique" con el objetivo final de permitir que el Cmdte tome más y mejores decisiones oportunas.

(3) El proceso descrito brevemente en el subpárrafo anterior se construye basándose en una PIC estándar, tal como se explica en el manual de empleo táctico de GE, pero además requerirá de:

(a) Un entendimiento del estilo de liderazgo y procesos de toma de decisiones del adversario.

(b) Un conocimiento de las necesidades técnicas sobre un amplio arreglo de sistemas de info (SINFOR).

(c) Un conocimiento de las influencias políticas, sociales y culturales que trabajan en el AIM.

(d) La habilidad para conducir procesos altamente técnicos para producir plantilla de formas de acción de G-C^2.

(e) La identificación de los líderes claves, los que toman decisiones, de sus comunicadores y asesores adversarios y de un entendimiento profundo de sus antecedentes biográficos.

(4) Mucha de la información requerida debería ser reunida y mantenida rutinariamente en las base de datos del nivel nacional y estar disponible al inicio de las operaciones o al recibir la misión.

(5) Las acciones de la PIC que un Oficial de inteligencia cumpliría para apoyar las OI incluyen:

(a) Construcción de un plantilla del proceso de toma de decisiones del adversario.

(b) Entendimiento de la infraestructura de información del adversario.

(c) Análisis de las vulnerabilidades del adversario.

(d) Desarrollo de opciones.

(6) Construcción de una plantilla del proceso de toma de decisiones del adversario

Es el primer paso del proceso de PIC de la info, enfocándose en el desarrollo del entendimiento de los perfiles de liderazgo y personalidad de los que toman decisiones en el adversario (los principales o los más críticos); incluyendo como ellos usan la info para tomar decisiones, como interactuan conforme las organizaciones toman decisiones y

como ejecutan estas decisiones. Este pasó será enlazado al objetivo final de las OI, que es encontrar la manera para: crear una respuesta deseada en el proceso de toma de decisiones adversario, crear una ventaja militar relativa o alcanzar el estado final deseado de una operación militar.

(7) Entendimiento de la infraestructura de info del adversario

Es el segundo paso del proceso de PIC de la info, que describe como fluye la info dentro de la unidad, organización y estructura. Este análisis incluye la interface humana como una forma válida de distribución de la info y no está limitado a solo la distribución tecnológica. El entendimiento de como fluye la info adversaria fuera de la unidad, organización o estructura, también debe desarrollarse para su empleo por el Cmdte, incluyendo el entendimiento de los ambientes local, nacional, continental y global. El personal de G-5 (asuntos civiles) pueden apoyar en este proceso.

(8) Análisis de las vulnerabilidades del adversario

(a) Es el paso siguiente, donde se analiza la plantilla de toma de decisiones y la plantilla de la infraestructura para determinar vulnerabilidades adversarias, las que pueden ocurrir en dos niveles.

1. Primero, se identifican sistemas vulnerables que pueden explotarse para causar el efecto deseado sobre el proceso de decisión.
2. Segundo, se determina el mecanismo apropiado de ataque y puntos de entrada especificas (edificio, piso, vía aérea, etc.)

(b) Luego el análisis de vulnerabilidades se extiende para incluir a los daños colaterales que pueden causar la acción de G-C^2 sobre el ambiente operativo. Por ejemplo, una acción de ataque sobre el C^2 adversario podría ser la destrucción de su infraestructura de energía eléctrica, sin embargo el costo estratégico (político, diplomático, etc) de destruir esta capacidad podría sopesar las ganancias tácticas.

(9) Desarrollo de opciones

La plantilla de toma de decisiones y la plantilla de la infraestructura de info son combinadas para formar una plantilla de forma de acción de atq'-C^2. Se pueden desarrollar y analizar varias formas de ación para determinar la mejor manera para usar las OI que permita influir, apoyar o cumplir la misión.

e. Evaluación de daños de batalla (EDB)

(1) La evaluación de daños de batalla sirve para confirmar o negar apreciaciones de inteligencia previas y actualizar la PIC. El sistema de inteligencia evalúa continuamente la efectividad de las OI. Este EDB permite a los Cmdtes ajustar sus esfuerzos en las OI para maximizar sus efectos. Un aspecto importante de esta EDB de información es un análisis oportuno para determinar cuando es creada, en la estructura de C^2 adversaria, una vulnerabilidad explotable. Comparada a la forma como se mira los procedimientos convencionales de informar la EDB, en las OI la EDB no será tan aparente.

(2) La EDB de información no siempre será reportada en términos de destrucción física de un objetivo, su reto es que sean capaces de evaluar los efectos de nuestro esfuerzo sin el beneficio de la confirmación física. Estos afectos bien pueden ser tendencias, actividades y patrones en futuras acciones adversarias, pudiendo ser tan simple como una ausencia de actividad sobre una red C^2, combinada con un incremento del tráfico en cualquier otra red; reducidas trasmisiones en VHF/UHF asociado con observaciones del incremento del trafico de mensajeros a horario o especiales; o actividades de patrullas terrestres o aéreas, etc.

(3) La EDB de información también examina el daño colateral de las acciones que la G-C^2 pudiera causar a los sistemas no-militares y capacidades dentro del AIM de un Cmdte.

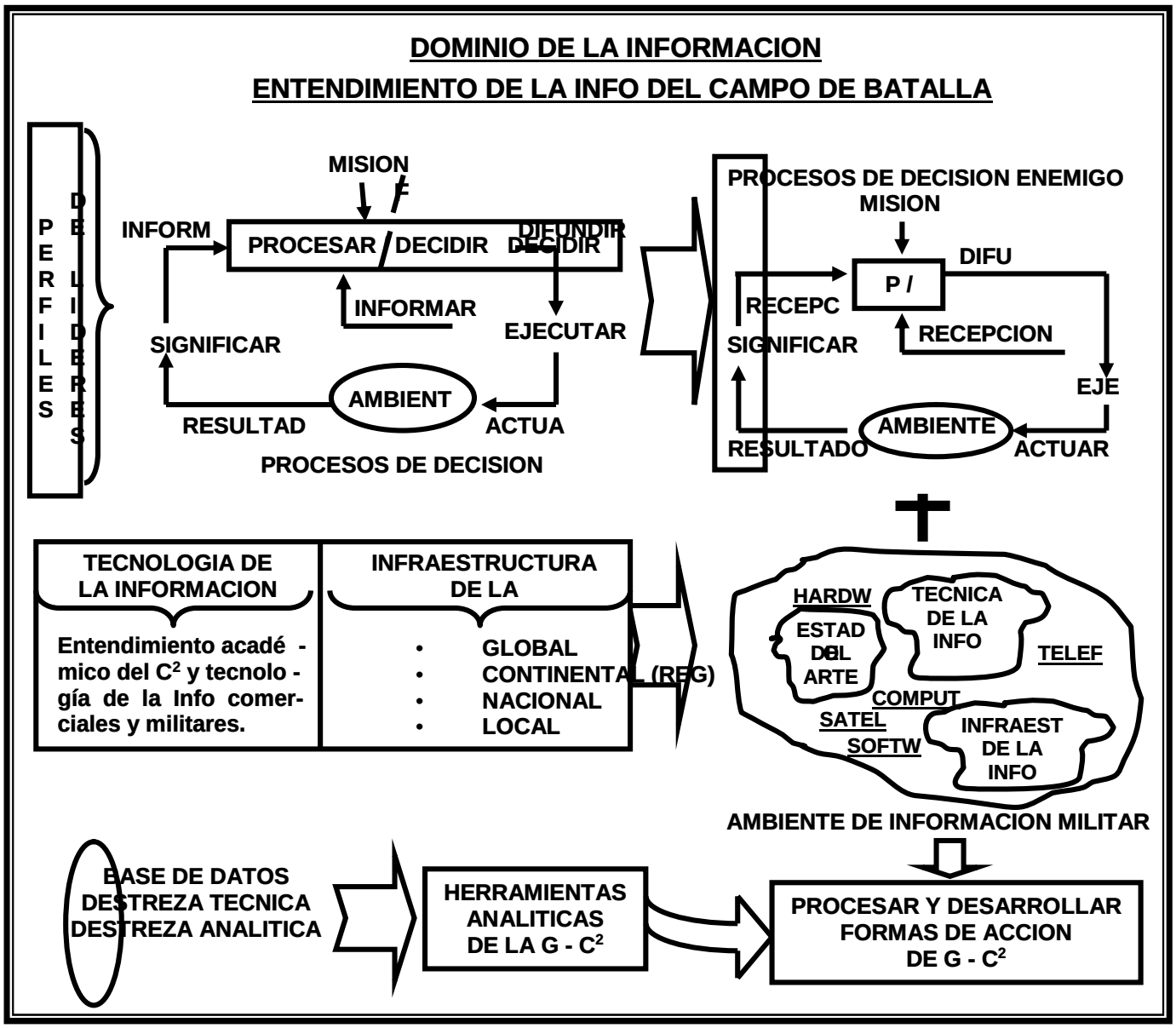

FIGURA 09: ENTENDIMIENTO DEL ADVERSARIO

CAPITULO 5
SISTEMAS DE INFORMACION (SINFOR)

SECCION I. FUNCIONES Y ROL DE LOS SINFOR

54. FUNCIONES DE LOS SINFOR

a. Las tecnologías del microprocesamiento, la miniaturización, las comunicaciones y el empleo de plataformas espaciales (satelites); se han combinado para permitir la conformación de info e inteligencia en tiempo casi real, la toma de decisiones distribuida y una rápida ejecución de órdenes desde una amplia variedad de fuerzas y sistemas para un efecto concentrado.

b. Los SINFOR permiten al Cmdte "ver y entender" su espacio de batalla, comunicar su intención, liderar sus fuerzas y difundir info pertinente sobre todo su canal de comando y su zona de operaciones. Los SINFOR efectivos, militares y no-militares, ayudan a un EM obtener la info correcta en el lugar correcto a tiempo para permitir a su Cmdte tomar decisiones calificadas y llevar a cabo acciones apropiadas.

c. Los SINFOR consisten de la infraestructura completa, organización, personal y componentes que reúnen, procesan, almacenan, trasmiten, proyectan, muestran, difunden y actúan sobre la información. Los componentes se refieren a las máquinas, procedimientos manuales o automáticos y sistemas operativos asociados.

d. La reunión, el procesamiento, el almacenamiento, la trasmisión, la difusión y la proyección de la info; constituyen las funciones que cubren todos los aspectos de la organización, proporcionando a los cmdtes un cuadro exacto, relevante y común, así como una conciencia situacional común. Consecuentemente, un cmdte debería considerar a su EM como parte del SINFOR porque su función jefatural es planear e integrar las OI.

e. Las SINFOR asimismo reúne, transportan, procesan, difunden y protegen la info en apoyo a las necesidades de info críticas del cmdte (NICC); posibilitándole emplear la info con efectividad para mantener una visión exacta de su espacio de batalla, coordinar las actividades de sus fzas tácticas y ayudarlo a conformar su AIM.

f. Los SINFOR apoyan directamente al comando de batalla, sin embargo, todos los aspectos de la guerra terrestre (opns, logística, planeamiento, inteligencia, etc) dependerán de una receptiva infraestructura del sistema de información. Los SINFOR deben ser capaces de apoyar simultáneamente el despliegue operacional actual y las contingencias futuras. La interoperatividad y la flexibilidad son características críticas de cualquier SINFOR, especialmente cuando deban conducirse operaciones conjuntas empleando sistemas operacionales o estratégicos.

55. ROL DE LOS SINFOR

a. El rol de los SINFOR es proporcionar la infraestructura que permita al ejército interfacear con la infraestructura de info global (IIG), posibilitando la integración de todas las actividades de las OI.

b. Los SINFOR deben conformar una arquitectura que permita:
   (1) Apoyar los procesos de los EEMM
   (2) Apoyar los procesos de toma de decisiones

(3) Proporcionar un cuadro común relevante que ayude a sincronizar la aplicación de la fuerza.
(4) Enlazar a los cmdtes y sistemas de armas asociados
(5) Apoyar las capacidades del atq´-C^2 y protección de C^2.

c. El desarrollo acelerado de las tecnologías de la info ha creado nuevas técnicas para manejar, transportar, procesar y presentar los datos, que incluye tecnologías de base de datos de imágenes, vídeo, gráficos a color, calcos digitales y mapeos digitales. Por otro lado, la evolución de la tecnología de la info ha desarrollado las comunicaciones satelitales, tecnologías de redes y computadoras e infraestructuras de sistemas de info militares y no-militares, que pueden combinarse para proporcionar al cmdte una capacidad de búsqueda global.

d. Finalmente, la arquitectura de las comunicaciones y la automatización permitirá un apoyo de C^2 modular para la fuerza confeccionado o estructurado durante cualquier fase de una opn. Hay que tener presente que hoy en día, las opns militares toman lugar en un ambiente global que demanda info de todas sus fuentes y los SINFOR militares y no-militares proporcionan esa capacidad global que apoya a los cmdtes y a sus unidades a través de todo el rango de esas opns.

e. En el Anexo 03, se detallan las consideraciones para el planeamiento de los sistemas de información.

SECCION II. CONCEPCION Y DESARROLLO DE SINFOR MILITARES Y SINFOR NO-MILITARES

56. CONCEPTUALIZACION DE SINFOR MILITARES

Los SINFOR militar son aquellos que integran y desarrollan, en campaña, las comunicaciones y los sistemas automatizados del campo de batalla, para enlazar funcionalmente a cuarteles generales estratégicos, operacionales y tácticos; con la finalidad de maximizar las redes de info disponibles a través de una conectividad perfecta así como una interoperatividad de C^2. La arquitectura de los SINFOR militar deberá establecer relaciones en los niveles estratégico, operacional y táctico, para estructurar los diferentes elementos distribuidos (apoyo de info de otros institutos, apoyo de inteligencia, apoyo de personal, apoyo de info logística, facilidades de comunicaciones, etc) en una red integrada, interoperable y cohesiva.

57. SINFOR MILITAR PROPUESTOS

a. Sistema de C^2 global conjunto.- Sería el principal sistema de información de C^2 nacional y estratégico de combate, que sería la interface con el sistema global de C^2 del ejército. La responsabilidad de la concepción, diseño y desarrollo de este sistema estaría en el comando conjunto de las fuerzas armadas y demandará el desarrollo de fundamentos doctrinarios comunes y de TTP´s de empleo de sistemas de comunicaciones, de automatización, de programas y de personal estandarizados. Adicionalmente, demandará la creación de cursos de capacitación y entrenamiento conjunto de comunicaciones y automatización en todos los estamentos de personal (oficiales, tcos, suboficiales y tropa especializada) con una estructura

curricular diseñada y actualizada constantemente de acuerdo a las exigencias tecnológicas del momento.

b. Sistema de C^2 global del ejército (SC^2 GE).- Que se diseñaría básicamente para servir al instituto desde época de paz, para apoyar a comandos mayores por encima del escalón ejército de operaciones, pero con la flexibilidad suficiente de adaptarse para servir al cmdte del componente terrestre en un teatro de opns. Deberá ser interoperable con los SGC^2 de otros institutos (Para mayor info ver Manual de Empleo de Comunicaciones Satelitales en el Ejército Ed 1999 párrafos 89 al 91).

c. Sistema de Comando de batalla del ejército.- Que se constituiría en el principal SINFOR de C^2 de combate del ejército, empleando un mixtura de instalaciones fijas y semifijas, así como redes móviles, dependiendo de los subsistemas empleados (satelitales fijos o móviles, red de fibra óptica, redes inalámbricas radiales, redes telefónicas, etc). Este sistema integrará vertical y horizontalmente los niveles operacional y táctico, siendo interoperable con el SGC^2 para todo el rango de las funciones de los sistemas operacionales del campo de batalla (SOC´s) y proporcionando conectividad para bases de datos de info de combate y procesos de info perteneciente a cada SOC. Este sistema comprende además del SGC^2, al sistema táctico de C^2 del ejército y a los sistemas de comando de combate de división y menores:

   (1) Sistema de C^2 táctico del ejército

      (a) Este sistema estaría enlazado directamente al SC^2G del ejército y proporcionaría el esquema para la conectividad precisa desde el nivel GU al EO. La intención de este sistema es integrar las diversas funciones de los SOC´s en una sola infraestructura coherente y precisa.

      (b) El primer reto será el desarrollo de capacidades de una internet táctica para establecer el uso y distribución de las nuevas posibilidades de las OI que hoy en día son posibles, debido a que el ejército ha iniciado la digitalización de todos sus sistemas de comunicaciones y muchas armas y servicios están introduciendo el empleo de sistemas digitales en sus unidades tácticas.

      (c) Esta internet táctica deberá contar con arquitecturas operacional y de SINFOR; la arquitectura operacional será necesaria para la conectividad de los elementos de la fuerza y por el tipo y volumen de info digital conformada por los elementos dentro de la fuerza; y la arquitectura del SINFOR será para hardware y software específico que provea conectividad y difusión de info del cmdo de batalla. Las dos arquitecturas envolverán versiones para que usuarios predeterminados intercambien necesidades de info a través de la fuerza.

      (d) Cada nodo de la internet táctica deberá poder proporcionar servicios de información mientras se está en movimiento. La administración de la red deberá ser una característica importante de la internet táctica y será altamente crítica para el éxito de la entrega de info a través del campo de batalla, posibilitando al administrador de la info táctica monitorear y seguir a los usuarios tácticos sobre el campo de batalla. Cada nodo proveerá una

herramienta para asesorar en la configuración dinámica que las redes de información del cmdo de batalla necesitan para conducir sus OI tácticas.

(2) Sistemas de comando de combate de división y menores (SCCDM)

(a) En términos cortos; el SCCDM empleará los sistemas de posicionamiento y navegación (GPS) y las comunicaciones sobre: sistemas de radio monocanal terrestres, tierra-aire-tierra, sistema de reporte de ubicación posición computado (EPLRS: enhanced position location reporting system), equipo terminal móvil de usuario (ETMU) y red de paquete táctico (MSE/TPN: mobile subscriber equipment/tactical pocket nerwork).

(b) Estos sistemas formarán una red integrada que moverá la información (datos) entre los escalones superiores y subordinados (verticalmente) y entre organizaciones adyacentes o vecinas (horizontalmente), sin necesidad de tener que ser enrutadas a través del PC o cuartel general de la GU.

(c) Los SCCDM deberán proporcionar conectividad digital desde el PC de la división hasta los sistemas de armas. La integración de los sistemas GPS, radios monocanal/EPLRS (o TACTER's) y MSE/TPN; para conformar una red homogénea y sistema de sistemas constará de:

1. **Terminales tácticos (TACTER)**.- Una familia de computadoras de tamaño laptop conectada a equipos de navegación y radios, para proveer procesamiento y posibilidades de proyección o visualización a plataformas sin un procesador interno.
2. **Internet táctica**.- Sistemas de comunicación de campo de batalla en red, empleando protocolos de internet comerciales.

58. SINFOR NO-MILITARES

a. La tecnología de la info está creciendo exponencialmente y transformando el modo como el mundo conduce sus negocios, su diplomacia y la guerra; requiriendo que los cmdtes tengan una visión más amplia y externamente orientada de todas las fuentes de SINFOR cuando ejecute OI. Las infraestructuras de los sistemas de comunicaciones civiles están mejorando tecnológicamente en cuanto a su movilidad y digitalización, que aunado a las mejoras en las armas y sensores dirigidos con energía electromagnética; continuarán reduciendo los factores de tiempo y espacio, y demandaran ritmos de opns más rápidos.

b. Los avances sin precedentes en la tecnología de los SINFOR continúan perpetuando una explosión global de las redes de info de naturaleza comercial o no-militar; creando una telaraña (web) global o "infoesfera de info" y provocando importantes cambios en la tecnología de las comunicaciones de radiodifusión, en la tecnología de computadoras y software; y en las tecnologías basadas en el uso del espacio (plataformas satelitales).

c. La naturaleza global y la velocidad de las difusoras de noticias pueden elevar los eventos de las opns militares, aparentemente oscuros; a un nivel de espectáculo internacional, creando un mercado para las noticias

conocido como “infotainmment”. El número de actores y participantes en el AIG está creciendo rápidamente y conformando nueva info sobre redes de computadoras. Por otro lado, los avances en la compresión de datos y comunicaciones celulares están proporcionando una mayor libertad de enlaces de comunicaciones a los individuos en cualquier parte del mundo, posibilitando también que los soldados de manera individual e independiente de los medios castrenses busquen enlazarse con sus hogares u otros destinatarios usando internet o fuentes de difusión y publicación para mantenerse informados.

d. Las fuentes potenciales de info inmediata, así como el número y variedad de influencias del AIM (intencional y/o inadvertida) se están multiplicando rápidamente y sus efectos acumulativos alterarán la forma de las organizaciones y la arquitectura de C^4 I de tal manera que está llegando a ser evidente:
   (1) Las redes están, en muchos campos, suplantando las jerarquías tradicionales como un concepto mayor de organización.
   (2) En el mundo de los negocios, la mayor conectividad y el acceso a la info en todos los niveles está eliminando muchas de las funciones de monitoreo o control realizado por administraciones intermedias.
   (3) Nuevas formas de pensar y operar serán necesarias, ya que los elementos que están en un nivel relativamente bajo en una organización ahora cuentan con info para tomar y ejecutar decisiones
e. Al igual que otros ejércitos del mundo, nuestro ejército deberá confiar y depender de muchos de los elementos del AIG sobre los cuales no se tendrá control y que constituyen los SINFOR no-militares, entre estos elementos tenemos:
   (1) Sistemas telefónicos públicos, sistemas de correos y postales
   (2) Sistemas de comunicaciones satelitales comerciales.
   (3) Receptores comerciales GPS
   (4) Sistemas de energía eléctrica que soportan las redes de info
   (5) Software aplicativos desarrollados comercialmente.
   (6) Medios noticiosos comerciales e internacionales (cadenas de noticias)
   (7) Bases de datos de acceso público.
f. La disponibilidad de SINFOR no-militares ofrecen a menudo al cmdo medios alternos para satisfacer sus necesidades informacionales de C^2, pero sólo después de una evaluación cuidadosa de los riesgos de seguridad. Como un beneficio adicional, el empleo de SINFOR no-militares puede reducir la necesidad de desplegar paquetes de SINFOR militar. El empleo operacional de un sistema de info no-militar permite a los planificadores compensar la falta de algún sistema y enfrentar el surgimiento de necesidades de info en las etapas iniciales de despliegue.
g. El G-6/S-6 será responsable por la estandarización del software y equipamiento no- militar empleado en toda la zona de opns; sin embargo los planificadores tendrán que asegurar el despliegue de paquetes de SINFOR modulares implementando estándares abiertos, no-propietarios, comúnmente aceptados y protocolos para interfacear con sistemas no-militares.
h. Las unidades de nuestro ejército tendrán que enfrentar el reto de la digitalización del campo de batalla, en especial las necesidades de interfacear al operador del equipo con el sistema y la necesidad de

desarrollar efectivas estrategias de entrenamiento. El uso óptimo de los SINFOR no-militares, dependerá finalmente de la disponibilidad de operadores y líderes calificados quienes deberán estar constantemente entrenados en la tecnología avanzada de SINFOR y en el uso de herramientas y aplicaciones avanzadas de automatización.

SECCIÓN III. APOYO DE TELEMÁTICA A LOS SINFOR

59. FUNDAMENTOS DEL APOYO DE TELEMÁTICA

a. El planeamiento de Telemática incrementa las opciones del cmdte al proporcionarle el requisito de sistemas de apoyo de comunicaciones para pasar información crítica en momentos decisivos, equilibrando y explotando los éxitos tácticos facilitando las opns futuras.

b. El apoyo de comunicaciones debe diseñarse para acomodarse a cualquier situación de despliegue, interface y operar con equipos de otros institutos e infraestructuras comerciales para proporcionar una arquitectura de redes perfectamente adecuada para satisfacer todas las necesidades de C^2 y apoyo de la fza.

c. El apoyo de Telemática se basa en cuatro principios operacionales: continuidad, seguridad, versatilidad y simplicidad; los que a su vez tienen elementos que los sustentan (Ver figura 10 Principios de apoyo de Telemática). Estos principios soportan el flujo de información entre los elementos de la fuerza sin importar la función, instituto o lugar, asegurando que apoyo sea sistemático y consistente en el desarrollo de la red, promoviendo un efectivo C^2 y apoyando a otros elementos del combate. Mayor información sobre los fundamentos del apoyo de Telemática pueden encontrarse en el Manual de Organización y opns de EM de Com (Ed 1999) y en el Manual de doctrina general de apoyo de Telemática (en edición).

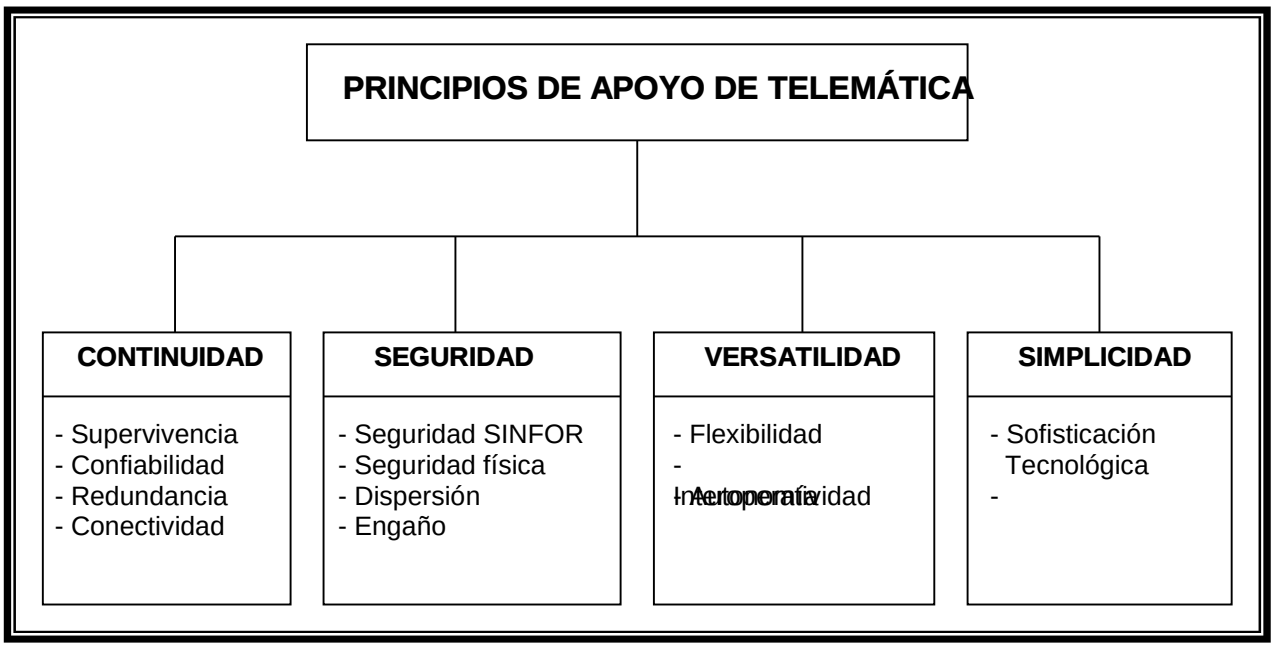

FIGURA 10: PRINCIPIOS DE APOYO DE TELEMÁTICA

60. TAREAS/MISION ESENCIAL DEL APOYO DE TELEMÁTICA

a. La información para el espacio de batalla requiere contar con sistemas de comunicaciones con capacidades de transferencia de info multigigabyte, protegida, perfecta, "end-to-end" y de procesamiento virtualmente en cualquier lugar y en cualquier momento. Esta capacidad debe ser un sistema de sistemas multimedia que transporte información de vídeo, imagen, datos y voz; para crear una infoesfera que el cmdte de batalla pueda introducir o extraer conforme él necesite visualizar la batalla desde su estado actual a un estado final exitoso.

b. Las tareas esenciales o misión de apoyo de Telemática para proyectar y construir la infoesfera son:

(1) Enlazar la fuerza a la infoesfera para alcanzar una conectividad global perfecta.

(2) Transportar info con sistemas de banda ancha y alta capacidad, optimizando el apoyo de Telemática terrestres y satelitales para conectar el cuartel general del ejército con todos los elementos y zonas del territorio nacional y eventualmente fuera de él.

(3) Extender el alcance de comunicaciones del combate y de los centros de opns del cmdo de batalla a través de comunicaciones en movimiento.

(4) Integrar los niveles de C^2 de la fza, integrando todos los SINFOR usados por los elementos del campo de batalla.

(5) Apoyar a los planes de campaña y de opns del combatiente buscando maximizar la efectividad del combate en todos los escalones.

(6) Sincronizar las opns de la fza, proporcionando los medios de enlace para que el cmdte pueda enfocar su máxima potencia combativa en el punto decisivo.

61. POSIBILITADORES DEL APOYO DE TELEMÁTICA A LAS OI

a. El objetivo del apoyo de Telemática a las OI es proporcionar al combatiente las posibilidades que necesita para obtener y compartir en tiempo casi-real; lo cual demandará la integración total de todas las funciones de administración de la info en un sistema de sistemas o sistema de cmdo de batalla que provea conocimiento basado en la info que sea adaptable y responda a los requerimientos de las OI del cmdte.

b. La arquitectura del sistema de comando de batalla del ejército (SCBE) deberá ser un juego de hardware y software de computador capaz de reunir; procesar, fusionar, manejar, transportar, difundir, mostrar/proyectar y proteger la info (status) y controlarla (intención, planes, órdenes). Las tareas esenciales o misión de apoyo de Telemática que posibilita las OI son:

(1) Digitalizar, comprimir y difundir información multimedia del comando de batalla en cinco categorías, usando un mayor ancho de banda y sistemas de transporte de alta eficiencia. Las cinco categorías son: controlar, monitorear, alertar, inquirir y explorar info crítica.

(2) Encriptar y proveer seguridad de información multinivel.

(3) Manejar las redes de info con software inteligente que distribuya dinámicamente toda la capacidad en demanda y luego enrute y difunda info.

(4) Mostrar/proyectar vía SCBE un interactivo tridimensional conocimiento basado en un cuadro común relevante.

62. TECNOLOGIA FUTURA DE COMUNICACIONES PARA APOYO A SINFOR

a. Conforme la tecnología avanza, la conducción de las opns continuará cambiando. Cada avance en la tecnología de la información permitirá:
   (1) Ayudar a los líderes a formar un cuadro más completo del espacio de batalla.
   (2) Generar decisiones potencialmente más rápidas y de mejor calidad.
   (3) Apoyar con mayor rapidez a la maniobra en términos de tiempo y espacio.
   (4) Incrementar la flexibilidad y agilidad de una unidad.

b. Sin embargo, la tecnología seguirá siendo sólo una herramienta que posibilitará el apoyo de Telemática a los SINFOR; la calidad de los soldados y líderes bien entrenados, continuarán siendo las piezas centrales para un exitoso planeamiento y operación de este creciente sistema de sistemas de información automatizados y digitalizados. Los ejemplos siguientes ilustran donde la tecnología de la información podría posibilitar un apoyo de comunicaciones eficiente a las operaciones militares en el siglo venidero:
   (1) Hoy, las redes de radiocomunicaciones tácticas existen de manera separada sin enrutamiento automático o interconexión entre redes. En un futuro campo de batalla digitalizado, la capacidad de una internet táctica posibilitará comunicaciones directas entre virtualmente todos los usuarios. Esto podría posibilitar un nivel completamente nuevo de integración, coordinación y sincronización horizontal que coexistirá con el actual sistema vertical (Ver figura 11 SINFOR horizontal y vertical).

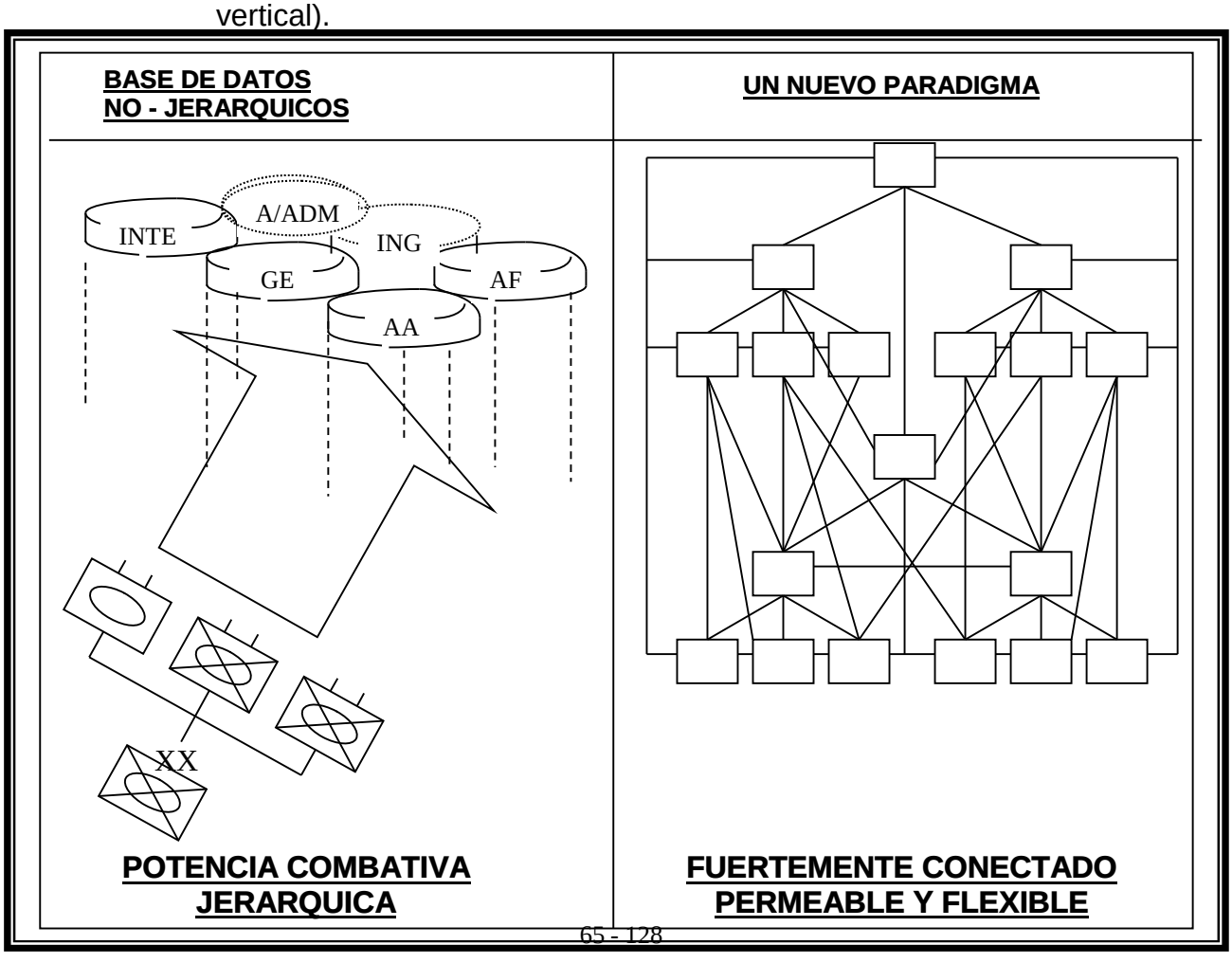

FIGURA 11: SISTEMAS DE INFORMACION HORIZONTAL Y VERTICAL

(2) Los satélites de difusión directa posibilitará un acceso global a la info en varios escalones en tiempo real o en tiempo casi real. Esto a su vez, posibilita un nuevo nivel de potencia y autoiniciativa para los escalones más bajos.
(3) La compresión de imagen y las tecnologías de trasmisión permitirán transferir imágenes y vídeo desde numerosos sensores y plataformas; posibilitando un mejor entendimiento del espacio de batalla para el planeamiento, ensayos y ejecución de la misión.
(4) Finalmente, la tecnología de multimedia posibilitará la presentación en tres dimensiones (3D) de imágenes y gráficos para ayudar al cmdte a visualizar su espacio de batalla para un entrenamiento, planeamiento, ensayo y ejecución más efectiva.

SECCIÓN IV. SEGURIDAD DE LOS SINFOR

63. RIESGOS CONTRA LA SEGURIDAD DE LA INFO

a. En el presente y en los próximos años nuestro ejército viene sobreincrementando su dependencia en los SINFOR automatizados; esto hace que la seguridad de la información (SEGINFOR) y de los SINFOR llegue a ser crítica. Desde época de paz hasta durante una guerra, las redes y sistemas a base de computadoras serán empleadas para procesar y transferir datos sobre logística, personal, administración, mantenimiento, finanzas y otras funciones de combate y apoyo de combate; que podrían ser vulnerables a un ataque.
b. A menudo, la internet será una plataforma de comunicaciones favorita para los intrusos, si es que la unidad está conectada a una red. Una vez que se ha obtenido el acceso a la red de comunicaciones y computador-servidor de alguna dependencia, pueden realizarse en ella una amplia variedad de métodos y técnicas para perturbar, influir o atacar al sistema. Algunos de los métodos más comunes incluyen:
   (1) Inserción de software malicioso a través de contratistas.
   (2) Seguimiento de los cambios del software de mantenimiento y actividades del sistema de opns.
   (3) Alternar los enlaces de acceso o rastrear las máquinas que atrapan info sobre el tráfico y “passwords”.
c. Estos intrusos pueden iniciar su acción durante época de paz o en cualquier momento de una opn. Es aun posible que un sistema militar especialmente los equipos de comunicaciones y computadoras que emplean microprocesadores, podrían venir de fábrica con una “bomba lógica” interna o virus programado para manifestarse en ciertas circunstancias o momentos.
d. Todos los riesgos mencionados en los subpárrafos precedentes y otros contra la info y SINFOR, imponen que los procedimientos y medidas de seguridad deban buscar preservar las SINFOR tanto activa como pasivamente en su integridad, confidencialidad y funcionalidad. Estas necesidades de protección incluyen medidas en tiempo casi real que detecten intrusos y alteraciones, así como la respectiva reacción y contracción para restablecer los SINFOR que el cmdte necesita para

apoyar su opn militar. Las tres principales medidas de seguridad que se emplean son:

(1) Procedimientos para asegurar la calidad de redes, programas y sistemas.
(2) Negar ingreso a personal no autorizado a las instalaciones.
(3) Protección de programas

64. PROCEDIMIENTOS PARA ASEGURAR LA CALIDAD

a. Los procedimientos para asegurar la calidad incluyen el control de la configuración de redes y programas; y, la reducción de corrupción inadvertida de datos y procesos.
b. Para proteger los SINFOR automatizados, el primer paso es entender la amenaza contra ellos. Estas amenazas contra la seguridad de los SINFOR son de dos categorías.

(1) Compromiso de datos e información.
(2) Negación, corrupción o perdida de servicio.

65. PROTECCIÓN CONTRA LA INTROMISION

La protección contra la intromisión en las redes de computadoras amigas es realizada mediante la negación a personal no autorizado a que acceda a estos sistemas. El gran porcentaje de intromisiones es debido a errores humanos; por lo que un adecuado entrenamiento y cumplimiento de la seguridad de las operaciones (SEGOPE) por los administradores, operadores y usuarios, serán las mejores medidas para combatir el compromiso del sistema. Adicionalmente, los administradores de los sistemas deben ser capaces de identificar y atrapar a los intrusos.

66. PROTECCION DE PROGRAMAS

Además de tener la capacidad para identificar y capturar a los intrusos, los programas de los sistemas deberían ser protegidos contra aquellos intrusos que intentan obtener info vital o dañar el flujo de información. Ningún plan de protección será perfecto y cualquier recurso de protección restauración será también finito, de ahí que los PP/OO y OO/OO deberán especificar las prioridades de los esfuerzos de protección.

SECCIÓN V. ADMINISTRACIÓN DE LOS SINFOR

67. ASPECTOS CONCEPTUALES DE ADMINISTRACION DE SINFOR

a. Existe un consenso general que los deseos por información del escalón superior excederán rápidamente la habilidad de un cmdte subordinado para proporcionarla de una manera oportuna. Los cmdtes en todos los niveles deben definir cuidadosamente sus necesidades críticas.
b. La Administración de los SINFOR consiste en la priorización de la información en un ambiente limitado de comunicaciones. El principal propósito de los SINFOR manuales y automatizados es lograr una ventaja de la info mediante el empleo y manejo de la info para una toma de decisión exacta y oportuna en cualquier tipo de opn.

c. El foco de un EM de batalla será balancear la tecnología disponible mediante el empleo de SINFOR que den al cmdte la información deseada en el tiempo correcto y en el lugar correcto.

68. PROCESO GENERAL DE ADMINISTRACION DE SINFOR

a. Toda la info que el EM proporciona está basada en la intención y concepto de operaciones del cmdte y apoyan además a las NICC. Estas NICC gobiernan la arquitectura de C^4 I así como su uso (Ver Manual de Organización y Operaciones de EM de Comunicaciones para más detalles sobre NICC).
b. Las NICC definen las necesidades de info del Comandante, enfocando así el apoyo del EM y de los SINFOR para una rápida obtención, fusión y análisis de info que de prioridad a las operaciones basado en el conocimiento. Los SINFOR aumentan los informes rutinarios y periódicos (establecidos por un POV de Unidad/GU) con necesidades específicas por información desde SOC´s u otras bases de datos.

69. ADMINISTRACIÓN TECNICA Y TACTICA DE SISTEMAS

a. El propuesto sistema de comando de batalla (SCB) del ejército deberá abarcar algunos sistemas y requerirá administración técnica con igual amplitud. Los SINFOR proporcionan un medio eficiente y rápido de recuperar info, posibilitando al EM desarrollar y mantener una singular, base de datos virtual (o lógica) que satisfaga las NICC actuales y anticipadas. Esto permitirá que el EM continuamente coordine, integre y sincronice las OI actuales y futuras. El SCB, que principalmente deberá trabajar en el nivel de clasificación SECRETO, deberá poseer tanto capacidad táctica como técnica en sus SINFOR.
b. Técnicamente, los dispositivos y aparatos de las redes del SCB deberían funcionar como un todo casi perfecto con enlaces redundantes. Los datos que fluyen entre computadoras no requerirán de acción intensiva de un operador; sin embargo el entendimiento, acuse de recibo e interacción con la acción recibida será generalmente un requerimiento del usuario.
c. La arquitectura de los SINFOR deberán cubrir todo un campo de batalla, de tal manera de posibilitar el comando y control de fuerzas. La arquitectura consiste de redes de área local (LAN´s: LOCAL AREA NETWORKS), redes de área amplia o global (WAN´s: WIDE AREA NETWORKS) y sistemas automatizados del campo de batalla (SAC´s); integrados en un único y casi perfecto sistema, sujeto solo a los requerimientos de la seguridad multinivel, tal como se describe en la figura 12 (Integración de la arquitectura de SINFOR de un campo de batalla).

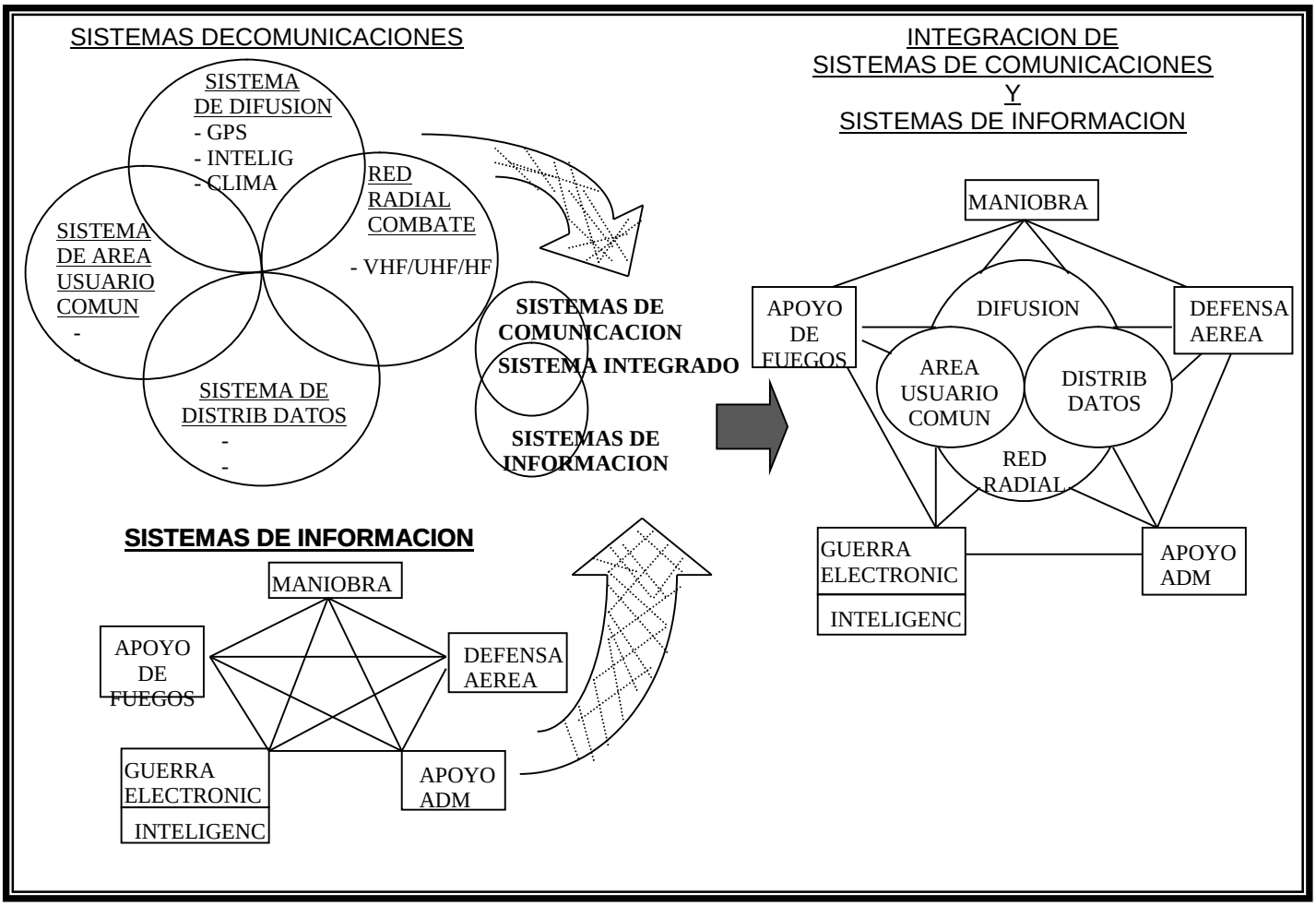

FIGURA 12: INTEGRACION DE LA ARQUITECTURA DE LOS SINFOR DE UN CAMPO DE BATALLA

d. Los SINFOR permiten al cmdte y a su EM distribuir info crítica entre fuerzas de elones superiores, subalternos, adyacentes y conjuntos. El tráfico de voz y la distribución de datos serán los principales métodos para pasar esta info; el primero de ellos incluye 3 tipos de trasmisión: usuario a usuario, conferencia y difusión; y el segundo incluye tráfico de mensajes en texto, facsímil, correo electrónico, datos de sistema a sistema y datos de posicionamiento y navegación (GPS).

e. La administración técnica de sistemas conecta todos los aparatos del SINFOR en una red segura multinivel que apoya al concepto de operaciones del cmdte y mantiene el nivel de seguridad correcta en cada nodo de red sobre todo el campo de batalla. Los requerimientos de esta administración técnicas incluyen:
   (1) Planeamiento de la red de SINFOR
   (2) Planeamiento de la conectividad de comunicaciones
   (3) Planeamiento de la seguridad de la red
   (4) Distribución de frecuencias
   (5) Control y monitoreo de la conexión de los aparatos de los sistemas de uno a otro sistema de comunicaciones que lo apoya.

(6) Reconfiguración de la red según se requiera de acuerdo a la situación táctica o fallas del equipo.
(7) Mantenimiento de la red.
(8) Maximización del rendimiento de la red.

f. Tácticamente, el flujo de información debe apoyar las necesidades del cmdte, quién conjuntamente con su EM deben tener la info que necesitan para planear, dirigir, controlar y coordinar una operación. La info debe ser segura y estar disponible rápidamente. La administración táctica de los SINFOR asegura que la info sea intercambiada dentro y fuera de la unidad, así como estar disponible de acuerdo a las necesidades de los cmdtes y sus EEMM para apoyar el plan táctico.

g. Dentro de cada SOC, el flujo de información, el procesamiento y el almacenaje son manejados de acuerdo a las necesidades de dicho SOC; para que la administración de todos los SOC´s sean administrados de acuerdo a las necesidades del cmdte para el nivel total de las fza. La administración táctica de sistemas incluyen:
(1) Planeamiento del intercambio de info
(2) Planeamiento de ubicaciones de bases de datos y duplicaciones
(3) Planeamiento de la continuidad de las opns (incluyendo seguridad)
(4) Control y monitoreo del intercambio de infos y transacciones de base de datos.
(5) Implementación continua de planes de opns de acuerdo a necesidades.
(6) Planeamiento en caso de degradación de la red.

SECCIÓN VI. ADMINISTRACIÓN DEL ESPECTRO ELECTROMAGNTICO PARA SINFOR

70. IMPORTANCIA DE LA ADMINISTRACIÓN DEL ESPECTRO ELECTROMAGNETICO

a. En un espacio de batalla dinámico, cada escalón de comando debe contribuir efectivamente al logro de una situación de dominio de la información. Para hacer esto, cada cmdte emplea el espectro electromagnético para sus propios propósitos, mientras previene de manera efectiva similar uso por un adversario.

b. El espectro electromagnético es un recurso valioso y finito, cuyo control será un factor vital para la digitalización; por lo que los cmdtes deberán tener un EM con conocimiento de dicho espectro. El G-6 tendrá la responsabilidad por la administración del espectro electromagnético en un campo de batalla, quién como administrador durante el planeamiento de las opns de info incluirá las consideraciones principales siguientes:
(1) Solucionar conflictos de frecuencias.
(2) Desarrollar instrucciones operativas de comunicaciones - electrónica.
(3) Desarrollar una lista de frecuencias restringidas
(4) Desarrollar lista de necesidades de ancho de banda solicitadas por inteligencia, G-C^2, AC, RP y elementos de comunicaciones.

71. ADMINISTRACION DEL ESPECTRO ELECTROMAGNETICO

a. Para ganar el control del flujo y contenido de la info, las unidades deben manejar efectivamente el espectro para reducir la probabilidad de interferencia electromagnética. Esto incluye el conocer las regulaciones y normas legales sobre la administración de frecuencias por parte del estado, en especial las frecuencias que el estado reserva para sus uso; así como acuerdo con naciones vecinas sobre uso de frecuencias.
b. También se debe tener presente las normas que emanan de la Unión Internacional de Comunicaciones (UIT), que distribuye las frecuencias de radio internacionalmente, registra la asignación de frecuencias y coordina la solución de interferencias.
c. Cuando una fuerza entra en operaciones, se crea una gran demanda porque la administración de frecuencias sea flexible y adaptable; ya que el adversario usará el espectro a su conveniencia, creando una fuente potencial de interferencia con las usadas por fzas amigas.

CAPITULO 6
PLANEAMIENTO Y EJECUCION DE LAS OPNS DE INFO

SECCION I. CONSIDERACIONES PARA EL EMPLEO DE LAS OI

72. CONSIDERACIONES GENERALES PARA EL PLANEAMIENTO DE LAS OI

a. El reto para los cmdtes en el siglo XXI será operar con efectividad en un ambiente dinámico conjunto y hasta multinacional contra una gran variedad de amenazas. El mantener la info con buena base ayudará al cmdte a enfrentar ese reto. Conforme las opns progresan o evolucionan a un ambiente total, la info y las opns de info (OI) llegarán a ser más importantes para el ejército en la ejecución de sus misiones para: impedir un conflicto, - imponerse a los oponentes, - reasegurar a fzas amigas y – proveer apoyo.

b. Los planificadores de las OI deben considerar las condiciones que afectan al ejército conforme él se despliega, enfocándose sobre su objetivo principal de alcanzar el dominio de la info, siguiendo un proceso de planeamiento que aplique correctamente los componentes de las OI en apoyo a las opns militares.

c. Las OI dependerán de una serie de consideraciones y condiciones que afectan a las opns militares, desde el despliegue hasta la culminación de las mismas. En la figura 13 se describe como las OI se aplican a través del espectro de opns y como el uso de los componentes de las OI, especialmente las opns de G-C^2, se incrementará en el tiempo de conflicto y de guerra.

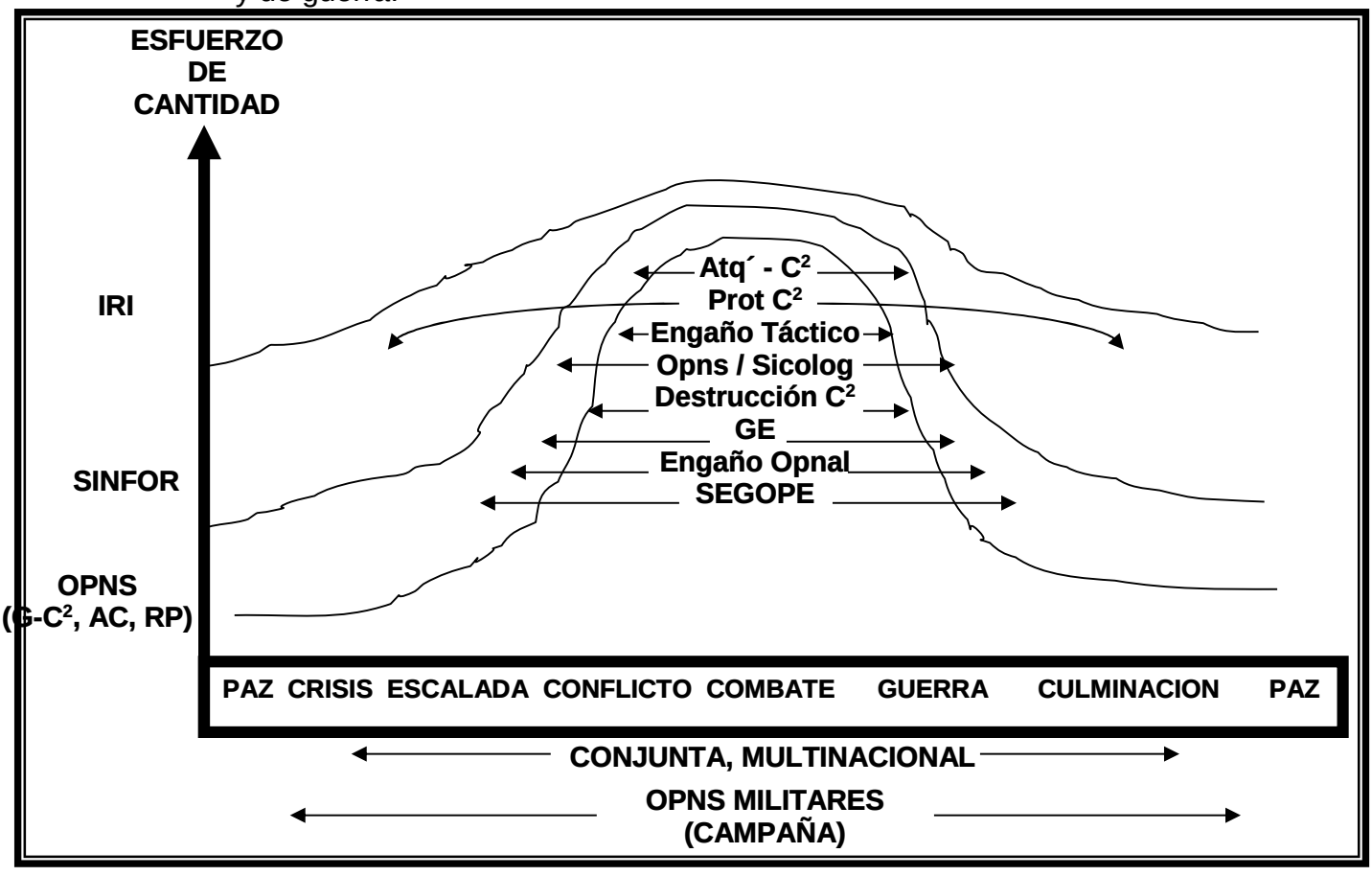

FIGURA 13: EMPLEO DE LAS OI EN EL RANGO DE OPNS MILITARES

73. LOS NIVELES DE LA GUERRA Y LAS OI

a. Los niveles de la guerra (estratégico, operacional y táctico) proporcionan un marco útil para el ordenamiento de las actividades de las OI dentro del espacio de batalla del cmdte, que lo ayudará a clarificarlas por escalones dentro de un teatro de opns (TO), las opns terrestres son conducidas como parte de una campaña mayor, integrada y conjunta.

b. Bajo la dirección de un comando nacional, un Cmdte de TO pone la campaña en movimiento, la que será apoyada por todos los elementos del poder nacional: sicosocial, económico, político y militar. La interconectividad y la interoperatividad de los SINFOR serán los elementos críticos que vincularán estas fuentes del poder nacional. Como se mencionó en el Capítulo 5, la conectividad de los SINFO será un prerequísito para el éxito en este ambiente multidimensional.

c. En el nivel estratégico

(1) En los escalones nacional y TO, el empleo de técnicas de OI ofrecen una serie de opciones estratégicas a ser consideradas. Estas opciones militares para atacar efectivamente un objetivo estratégico, mientras se minimiza los potenciales efectos devastadores del uso de armas convencionales, han crecido en importancia. Las OI del ejército ofrecen potencialmente tanto capacidad disuasiva como capacidad coercitiva en todos los niveles de la guerra.

(2) Los efectos de las OI pueden ser sobre un amplio espectro o puede ser sobre capacidades hostiles específicas. Igualmente las OI pueden eventualmente desarrollar sus capacidades de manera ofensiva o defensiva, apoyando a la estrategia nacional sobre la base de una variedad de combinaciones de atq' – C^2 y protec – C^2. Desde un punto de vista meramente técnico, el abanico de candidatos a ser considerados como objetivos para las OI y el rango de alternativas operacionales son virtualmente ilimitadas.

(3) Los cmdtes, en apoyo a los objetivos estratégicos nacional y del TO, son responsables por el empleo de todo el rango de sus posibilidades de info durante una guerra. Como parte de una estrategia nacional de G-I, el ejército puede ser misionado para emplear sus posibilidades para apoyar acciones directas e indirectas, es decir, fuera de un contexto puramente de campo de batalla.

(4) Las posibilidades de la información y de los SINFOR enlazan inextricablemente los tradicionales niveles de la guerra. Este fenómeno requiere que los cmdtes y EEMM en cada nivel entiendan la info obtenida, donde se necesita la info y los medios o conectividad necesaria para entregar y/o recibir esa info. Los sistemas de nivel nacional (de defensa y comerciales) están aumentando su capacidad de apoyar y mejorar las opns tácticas (info del clima, comunicaciones, imágenes, navegación).

(5) En muchos casos la conectividad es encontrada a través de otros institutos o empresas públicas y privadas (satélites, instituto geofísico, meteorología, etc). Los sistemas de guerra electrónica de HF, empleados en los niveles estratégicos y/u operacional con otros recursos conjuntos de G-C^2, podrían disminuir la confianza del oponente y su deseo de combatir antes del inicio de las opns. Finalmente, las OI necesitan estar coordinadas, integradas y

sincronizadas con el Plan de Campaña para alcanzar resultados decisivos.

d. En el nivel operacional
   (1) En este nivel, las OI ocurren a través de todo el rango de las opns desde época de paz hasta en conflicto. En época de paz apoya:
      (a) La disuación y la tranquilidad.
      (b) La conciencia situacional general
      (c) Evaluación y apreciaciones operacionales
      (d) Planeamiento de contingencias
      (e) El entrenamiento en apoyo al Cmdte y la preparación de actividades.
   (2) Durante el conflicto u hostilidades, las OI implementan actividades de G-C^2 en cada nivel de la guerra. Los continuos encuentros en OI ayudan al cmdte a lograr y mantener la iniciativa y posibilidades de sincronización operacional. Esto permitirá al cmdte controlar el ritmo de las opns para que las fzas amigas puedan con efectividad transitar desde la época de paz a situaciones y ambientes operacionales en tiempo de guerra. El dominio de la info en tiempo casi real, la habilidad para visualizar el campo de batalla, un flujo de info ininterrumpido y las posibilidades de reconocimiento y vigilancia intactas; constituirán los factores de éxito de la campaña operacional.

e. En el nivel táctico
   (1) En este nivel, los cmdtes usualmente cumplen sus misiones mediante opns de armas combinadas y las OI están a menudo limitadas en propósito. Mientras un cmdte de nivel táctico emplea todos los aspectos de las OI, a menudo el foco será el trastorno, dislocación o destrucción de los SINFOR o nodos enemigos, principalmente a través de la GE y la destrucción física. El cmdte mantendrá el acceso a sus SINFOR mediante la SEGOPE, la seguridad de los SINFOR y la protección electrónica (COCOME).
   (2) Otras aplicaciones de las OI en este nivel incluyen:
      (a) Planeamiento y ejecución de G-C^2
      (b) Proyección y construcción de la infoesfera.
      (c) Protección de la info amiga.
      (d) Establecimiento y mantenimiento del acceso usuario a la info del comando de batalla vía el futuro sistema de cmdo de batalla del ejército.
      (e) Instrumentar las OI y la visualización del campo de batalla.
      (f) Reunir y producir IRI.
      (g) Atacar el sistema de C^2 enemigo.
   (3) El dominio de la info es una condición táctica temporal que se alcanza a través de un proceso deliberado; que implica la construcción y protección del ambiente de información, reunión de inteligencia e información relevante, procesamiento y difusión de tal información; y enfocar el ataque contra el C^2 eno y sus “ojos y oídos”. El dominio de la información facilita la superioridad en la visualización del campo de batalla en un tiempo y lugar específico, creando una “ventana” de oportunidad que es como mucho momentánea. El cmdte debe aprovechar la oportunidad para ganar la ventaja a través de un

comando de batalla efectivo. Dos características son esenciales en este proceso:

(a) NICC.- El cmdte debe controlar la info o correrá el riesgo de ser abrumado o desorientado por ella. Las NICC pueden controlar la superabundancia de info y separar las Telemática verdaderas del ruido. Las NICC no pueden ser un concepto fijo; pues al igual que la PIC, debe ser precisa para asegurar la receptividad y dinámica para supervivir.

(b) Ritmo.- Es el tiempo dedicado al proceso de toma de decisiones tácticas. La ejecución debe ser dramáticamente comprimida; pero debido a que la ventaja del dominio de la info es alcanzada a través de una acción deliberada dentro de un espacio de batalla específico, el comando de batalla deberá estar mejor sincronizado para dar como resultados la creación de oportunidades que guíen el éxito.

(4) Las unidades tácticas, tanto de maniobra y de apoyo de combate, participar en las OI, dirigidas por sus cuarteles generales superiores. En algunas opns, las unidades tácticas realizan la selección como objetivos y ataque a: nodos de C^2, al engaño, al reconocimiento y vigilancia; y actividades de opns/sicolog enfocadas al apoyo de los OI totales del nivel TO.

(5) Con una visión expandida, los cmdtes tácticos anticipan las amenazas de desinformación, las opns/sicolog enas y rumores dentro de su comando, así como las repercusiones potenciales de la info pública dentro de su espacio de batalla. El establecimiento de un efectivo programa de info interno mejorará la moral de los soldados, reforzará la misión establecida de su unidad y apoyará con informes a los soldados y sus familias empleando medios exactos y precisos.

74. RESTRICCIONES Y LIMITACIONES EN LAS OI

a. Conforme los cmdtes y sus EEMM planeen, preparen y ejecuten las OI, será necesario una conciencia acrecentada de cómo darle forma a las opns y que éstas estén de acuerdo al AIM; ya que la info puede y de hecho será diferentemente interpretada por cualquier número de individuos o grupos, afectando la estructura política, social y económica de la vida de los individuos, organizaciones y hasta naciones; más allá del propósito e intención de la operación militar. Esta realidad crea un juego dinámico de restricciones y limitaciones que impactarán sobre las opns militares.

b. Operaciones asimétrica o híbridas son la norma como las estructuras de las fuerzas están ensambladas para enfrentar una amplia variedad de necesidades. Concordantemente, existen diferentes niveles de modernización dentro del ejército y entre las fuerzas u organizaciones de tareas conjuntas, las cuales emplean dispares tecnologías de información y de comunicaciones que afectan la continuidad e interoperatividad. Las posibilidades de las OI pueden compensar estas variantes, proporcionando a la fuerza la conectividad necesitada para operar con efectividad .

c. Las limitaciones estatutoarias; las leyes internacionales; las leyes, normas y reglamentos del estado; y, las reglas de encuentro; pueden limitar las opciones del cmdte con respecto a las OI. Las leyes y regulaciones, tales como aquellas que el gobierno dicta sobre el espectro de frecuencias,

información pública, etc; proveen ejemplos de acceso libre a la info y SINFOR intentando prevenir el mal uso o abuso de estas actividades. Las OI pueden aun ser más restringidas o más habilitadas conforme se establezcan nuevas leyes, reglamentos, acuerdos y/o protocolos; y conforme la comunidad internacional se ajusta al impacto de la explosión de la info.

d. La interferencia simple, la manipulación deliberada y la corrupción o destrucción de bases de datos o SINFOR, incluyendo los sistemas basados en el espacio (satelitales); han llegado a incrementar las actividades sensitivas y activas. La telaraña de info y su continuidad o su dislocación tiene implicaciones más allá del AIM, para abarcar dimensiones económicas, políticas y sociales. La competencia por una porción del espectro electromagnético, por parte de los sistemas satelitales, redes de comunicaciones inalámbricas terrestres y redes de computadoras; todas ellas sientan las bases de una etapa de potenciales interferencias tanto intencional como no-intencional.
e. Conforme el ejército se vaya moviendo e introduciendo en la era de la info, las características del espacio de batalla continuará cambiando; y los medios y métodos de conducir todos los tipos de operaciones también cambiarán. Los éxitos en cualquier ambiente operacional dependerá del liderazgo, disciplina, moral y entrenamiento profesional.
f. Las opns de hoy y del siglo XXI dependen y dependerán de la inteligencia y de los SINFOR más que antes, desde el nivel táctico hasta el estratégico para proporcionar info crítica sobre todos los aspectos de la situación amiga y enemiga. El flujo horizontal y casi perfecto, así como la integración de la info proporciona datos operacionales valiosos para apoyar al planeamiento y al comando de batalla.
g. Aunque el peligro de guerra total ha disminuido hoy en día, ella nunca desaparecerá completamente. El cmdte enfrentará siempre alguna incertidumbre sobre el dispositivo exacto de la fza ena, su orden de batalla, y opns en general, sin mencionar que tendrá algún grado de incertidumbre sobre las intenciones enas. Esa incertidumbre estará compuesta por oponentes ingeniosos (militares o no) e individuos exacerbados por las consecuencias de acciones no-intencionales o influencias de otras fuentes dentro del AIM del cmdte.

SECCION II. DOMINIO DE LA INFORMACION PARA LA TOMA DE DECISION

75. LAS OPNS DE INFO EN EL COMANDO DE BATALLA

a. El objetivo principal de las OI es ganar el dominio de la info, una ventaja relativa del proceso de toma de decisiones amigo sobre el del adversario; y emplear esa ventaja para mejorar y posibilitar a los elementos de la potencia combativa. Las OI son un fundamento esencial del conocimiento para la guerra de armas combinadas que apoyarán o actuarán para el comando de batalla.
b. Las opns del ejército están hoy en día profundamente afectadas por la info y las OI, en las funciones críticas del comando de batalla; y aunque éste seguirá principalmente siendo un arte, crecientemente viene confiando en

la habilidad para procesar info para moverse rápidamente a puntos críticos en el área operacional. Para alcanzar el nivel requerido de dominio de la info en la era de la info, el cmdte deberá tratar a las OI como trataría a cualquier otro elemento crítico de su poder de combate (potencia combativa); proporcionando orientación y dirección a su EM y a sus cmdtes subordinados.

c. El involucramiento personal del cmdte en el desarrollo de las NICC, hace de él el principal vehículo para asegurar que sus necesidades de info del comando de batalla sean satisfechas. Los avances en la tecnología de la info han hecho de la toma de decisiones y del control de las unidades, actividades más técnicas y cuantificables, aún cuando muchas de estas funciones permanecerán dentro del campo del arte y no de la ciencia. Los cmdtes deberán entender que nunca se tendrá toda la info crítica que necesita y cuándo él la quiera; por lo que liderar a soldados y unidades hacia el éxito mayormente segura siendo arte; consecuentemente, lo que un cmdte deberá buscar será emplear a las OI para retener una ventaja de info sobre su oponente.

d. El desarrollo de la tecnología digital ha mejorado el C^2, permitiendo al ejército tener la posibilidad de contar con cantidades inimaginables de información exacta y confiable; así como permitir a los cmdtes poseer un conocimiento detallado sobre eventos que ocurren dos o más escalones por debajo del suyo, al mismo tiempo que da a los subordinados más info sobre un cuadro mayor y sobre lo que estaría pasando en otras áreas o zonas de ese cuadro. Basado en ese cuadro común relevante (CCR), los cmdtes estarán mejor habilitados para integrar su poder de combate de manera continua y en tiempo casi real.

e. La tecnología y el tiempo no cambiarán algunos aspectos del comando de batalla. Los cmdtes y sus EEMM continuarán haciendo juicios en base a información un poco menos que perfecta; y probablemente ellos tendrán que inspiran a sus soldados para que realicen sus tareas superando el temor y fatiga, continuarán moldeando a sus unidades para que alcance un alto nivel de realización a través del entrenamiento, desarrollo del canal de comando, manejo personal, moral y un clima positivo de comando.

f. Elementos básicos del comando de batalla

Los 3 elementos básicos del cmdo de batalla están caracterizados por la continuidad y el cambio. Estos elementos son:

(1) Liderazgo.- Un continuo liderazgo del cmdte proporcionará propósito, dirección y motivación a los soldados y unidades. Los líderes estarán mejor preparados para tomar decisiones informadas, pero operarán dentro de una filosofía que no cambiará.

(2) Toma de decisión.- Estará facilitada por tecnologías de información muy mejoradas, el mantenimiento de un cuadro común relevante (CCR) sobre el cual basar sus decisiones y por ejercicios para líderes que mejoren la toma de decisión.

(3) Control.- Estará facilitado por mejores comunicaciones, que incluyen vídeo-difusión, enlaces de mayor capacidad, nuevas tecnologías de reporte de posición-localización (PLRS), mayor conciencia situacional, mapas electrónicos formados de manera remota, ayudas de apoyo a la decisión automatizados; y otras tecnologías de la info y procedimientos.

g. Retos dentro del comando de batalla

Los retos para los líderes serán proporcionar propósito, dirección y motivación a las fuerzas que pueden estar operando sobre grandes espacios, bajo gran presión de tiempo y en medio de situaciones complejas. Las implicancias específicas de las OI y como ellas se aplican al arte del cmdte incluyen lo siguiente:

(1) La identificación, la concepción y la comunicación del propósito de la unidad seguirá siendo un arte complejo, mayormente del dominio del cmdte. El entender la misión, la intención de los cmdtes dos escalones arriba y el concepto de la operación de una organización "padre", puede ser más fácil con comunicaciones mejoradas; sin embargo la expresión o aprobación de la misión reexpresada, la formulación de la expresión de la intención y la emisión de la decisión y concepto de opns, son aún funciones que el cmdte debe realizar por sí mismo.

(2) Una aproximación doctrinaria a las órdenes tipo – misión y/o a la toma de decisiones descentralizadas, no anticipan cambio. La habilidad para comunicarse a "control remoto" con sus cmdtes subordinados y EM por vídeo conferencia u otros medios electrónicos, no eliminarán la necesidad del cmdte de proveer dirección implícita a ellos. Sin embargo, la tecnología de la info mejorará el esfuerzo por proporcionar un CCR a través de los SOC´s y otras funciones en tiempo casi real. Durante las acciones críticas, el cmdte enfocará mucha de su atención y toma de decisión sobre su esfuerzo principal, por lo tanto será vitalmente importante confiar en que sus subordinados actuarán dentro de su intención y concepto de operación.

(3) Los cmdtes necesitan motivar a sus soldados, también como a sus EEMM y otros elementos, para cumplir tareas difíciles bajo circunstancias duras y peligrosas; ellos continuarán inspirando a su subordinados mediante comunicaciones frente a frente y presencia física. Aunque pudiera ser dificultoso, los cmdtes necesitan aún posicionarse donde puedan "ver el campo de batalla" y donde sus tropas puedan verlo. Asimismo, los cmdtes establecen relaciones interpersonales con sus EEMM y cmdtes subordinados, contribuyendo a la unidad de esfuerzo y fomentando relaciones personales entre comandos para promover la confianza mutua, la cooperación, las comunicaciones abiertas y el trabajo en equipo en las opns. La retroalimentación informal será también útil.

(4) Las incertidumbres siempre existirán. El cmdte puede saber lo que el eno está haciendo en un momento, pero rara vez sabrá porque. Un juicio sensato del comando determinará que puede hacer el eno mañana. Por otro lado, no importará que tan bien conoce el cmdte el estatus de sus fuerzas hoy, él necesita hacer juicios sobre cuales pueden ser sus condiciones mañana; no importará cuanta info el cmdte obtenga antes de tomar una decisión, las incertidumbres aún subsistirán, existirán vacíos de info e info no-cuantificable.

(5) La habilidad para procesar info a través de la administración del riesgo posibilitará a los cmdtes evitar riesgos innecesarios. Identificando, analizando y seleccionando medidas de control para manejar los riesgos; dará al cmdte máxima protección a su fuerza.

76. RESPONSABILIDADES DE EM PARA LAS OI

a. Para facilitar las OI, el cmdte establece responsabilidades de EM para el planeamiento y ejecución. Dependiendo de la situación, el planeamiento de las OI puede ser una tarea compleja o una función relativamente de rutina del EM; sin embargo la organización de una celda especializada extrayendo expertos seleccionados del EM de coordinación y del EM especial con oficiales de enlace y otros refuerzos posibles de comandos subordinados; puede mejorar el planeamiento de las OI. Una cantidad de técnicas y una variedad de arreglos estarán disponibles para cumplir estas responsabilidades, que se mencionarán en subpárrafos siguientes.

b. Miembros del EM

Los miembros del EM actual pueden integrar las acciones de las OI en la operación. Este enfoque emplea los actuales procedimientos de EM, sus procesos y técnicas para planear, coordinar y sincronizar las OI con la operación táctica. La opción probable para una fuerza no modernizada o parcialmente modernizada será la designación de un representante de EM para supervisar estas acciones.

c. Grupo de proceso orientado

Un proceso orientado o grupo de tarea “ad hoc”, liderado por el C-3/G-3, puede integrar y sincronizar las acciones de las OI. Este enfoque es similar al que se emplea para determinar objetivos o para el ataque en profundidad. Esto también es un enfoque viable para fzas particularmente modernizadas o fzas no modernizadas que entren a un combate complejo o ambiente de no combate, donde existen amenazas y/o un número de capacidad de OI.

d. EM de batalla para OI (EMBOI)

Este enfoque visa constituir un EM que integre las acciones de las OI y podría ser aplicable a fuerzas totalmente modernizadas. El EM estaría constituido por todos los miembros del EM con una responsabilidad funcional dentro de las OI, tales como: Telemática (G-6), apoyo de fuegos (CAF), AC (G-5), RP, SEGOPE (G-2), GE (Oficial de GE), Opns/sicolog (G-3 y Oficial de opns/sicolog) y engaño militar (G-3).

e. Administrador de la información

(1) Desde que las opns de info son sólo una faceta de una operación mayor el C-3/G-3 será el administrador principal de la info. Él bosqueja y monitorea el rendimiento y responsabilidades del EM en el procesamiento de la info para apoyar al flujo del conocimiento y a las OI, asegurándose que el EM reúna, analice y presente info que satisfagan las NICC. Las solicitudes específicas por info provenientes de los SOC´s u otras fuentes de info de base de datos serán generados para llenar necesidades específicas. Los informes de rutina hacia el EM se emplearán cuando las necesidades de info permanecen estables durante las opns.

(2) El C-3/G-3, dentro de su responsabilidad total de EM para integrar las OI en el P/O, usualmente designará a un individuo encargado de

todas las acciones de OI. Los miembros claves que participarán en la coordinación e integración de las OI incluyen al C-2/G-2, C-6/G-6, CAF, C-5/G-5, RP, Oficial de GE, especialista en engaño, especialista en SEGOPE, Oficial de Opns/Sicolog y a personal proveniente del C-4/G-4.

f. Elementos de actividad de G-I del componente terrestre (EAGIT)

(1) Al nivel operacional, la G-C^2 demandará que los cmdtes desarrollen y mantengan miembros del EM técnica y operacionalmente eficientes en este tipo de opns. Hacer esto es una empresa compleja que exigirá entrenamiento extensivo, educación profunda y mucha experiencia en el trabajo con otros institutos, dependencias públicas y privadas y comandos conjuntos. A fin de mejorar la capacidad del componente terrestre de un TO, para conducir OI, será deseable la creación u organización de un elemento permanente que se podría denominar Elemento de actividad de G-I del componente terrestre (EAGIT), que actuará como punto focal para la G-I y la G-C^2 proporcionando apoyo de EM operacional al cmdte del componente terrestre.

(2) Este elemento consistirá de una mixtura de especialistas en opns/sicolog, engaño militar, SEGOPE, GE e inteligencia del ejército junto con miembros de otros institutos como sea necesario, quienes tendrían la responsabilidad de planear, coordinar y ejecutar la G-I/G-C^2 en ambientes conjuntos.

SECCION III. PROCESO DE PLANEAMIENTO DE LAS OI

77. PASOS DELPROCESO DE PLANEAMIENTO DE LAS OI

El proceso de planeamiento de las OI consiste de cinco (05) pasos básicos que se aplican a través de los tres (03) componentes de los OI (opns info propiamente dichas, IRI y SINFOR). Estos pasos son:

a. Análisis de la misión
b. Priorización
c. Concepto de operaciones de OI
d. Ejecución
e. Retroalimentación

Estos pasos serán tratados en párrafos separados dentro de esta sección y en la figura 14 "(de la página siguiente)" se ilustra el proceso total.

78. ANALISIS DE LA MISION (PASO 1)

a. El primer paso del proceso comienza con el análisis de la misión y formulación del concepto de opns total, donde se considerará como las OI pueden contribuir al cumplimiento de la misión del cmdte. Bajo la dirección del C-3/G-3, el EM analiza la misión y concepto de opns del comando para derivar un concepto de OI. El EM debe considerar tanto el atq´- C^2 como la prot C^2. Será esencial la flexibilidad, conforme el apoyo de las OI pueda cambiar el curso de una opn total.

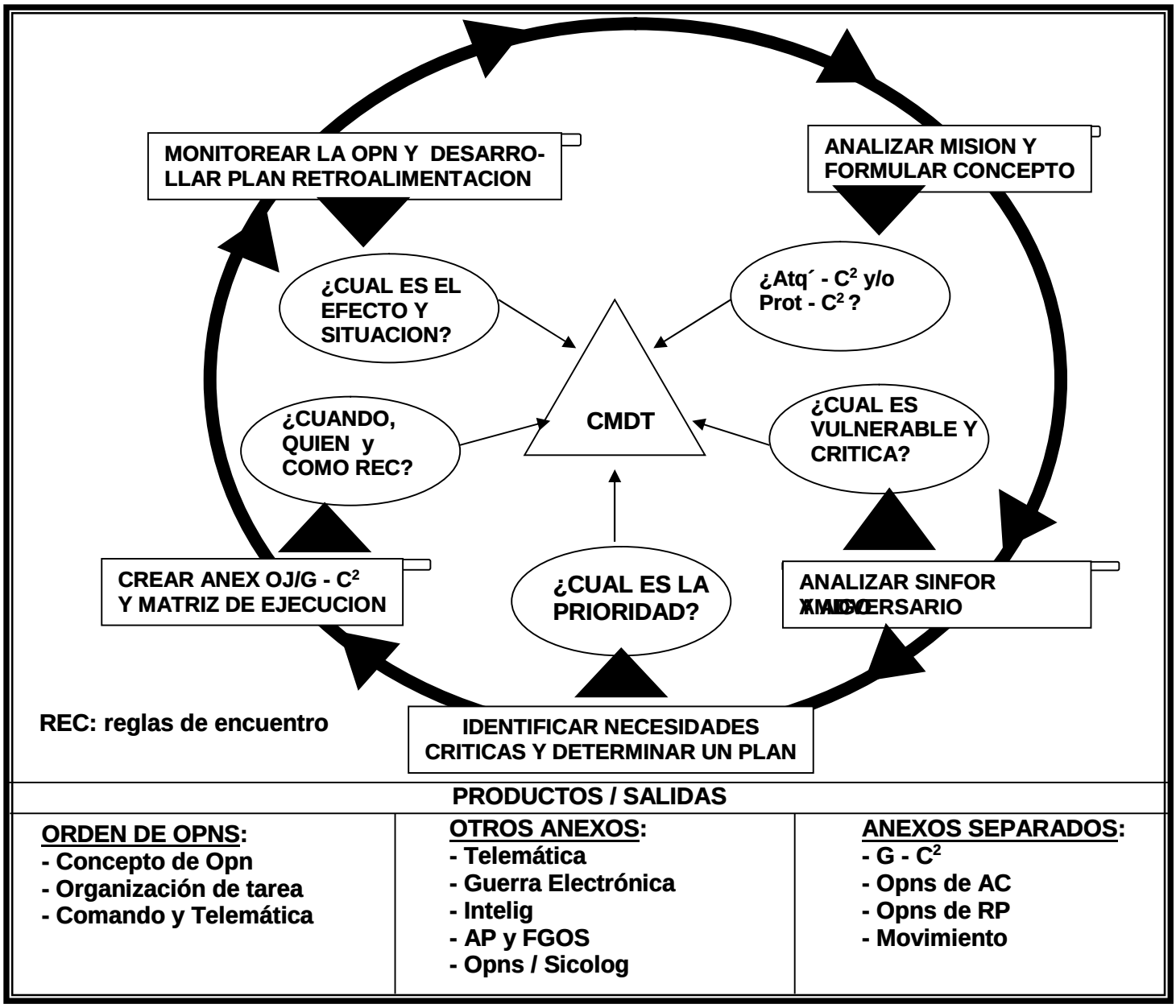

FIGURA 14: PROCESO DE PLANEAMIENTO DE LAS OI

b. Durante este paso, el EM examina los SINFOR amigo y enemigo dentro del contexto del AIM del cmdte. El EM determina las capacidades de ambos lados que se requieren para operar efectivamente, así como establece los requerimientos y condiciones necesarias para alcanzar el dominio de la información; considerando las influencias y posibilidades de los SINFOR no-militares más allá del tradicional control militar tales como las redes de telecomunicaciones del lugar, la radio y televisión, las redes de computadoras (internet o worldwide web) y los medios de noticias; que pudieran influir sobre la opn. Este examen producirá una lista de nodos críticos y análisis de vulnerabilidades:

(1) El análisis del atq´- C^2 identificará los sistemas de C^2 adversario de interés para el G-C^2 y determinará el C^2 crítico y nodos de atq´- C^2 en aquellos sistemas. El atq´- C^2 se enfocará en incrementar el valor de

la identificación de las vulnerabilidades de objetivos claves para la acción ofensiva.

(2) El análisis de la prot-C^2 se enfocará sobre las posibilidades adversarias para detectar, localizar y atacar los nodos de C^2 críticos amigos y para perturbar su proceso de toma de decisiones. Al igual que con el atq´-C^2, la inteligencia juega su mayor rol proporcionando info sobre las capacidades de los sensores adversarios, de selección de blancos y de sus medios de ataque. El EM considera la destrucción física, la perturbación electrónica, la intromisión, el engaño y los medios de opns/sicolog que el adversario pudiera disponer. El resultado será una lista de nodos críticos vulnerables y procesos que deben protegerse.

79. PRIORIZACION (PASO 2)

a. El segundo paso del proceso de planeamiento de las OI es priorizar los nodos críticos y vulnerabilidades amigas y enemigas. Esta parte del proceso desarrolla los objetivos potenciales para el atq´- C^2 y prot-C^2 y asegura la eliminación de discrepancias de sus efectos integrados.

b. Para propósitos de atq´- C^2, los nodos críticos para más de un sistema adversario pueden anular la criticabilidad, con más nodos críticos que son menos vulnerables recibirán una prioridad más baja. Las prioridades deberían ser balanceadas y moverse entre atq´- C^2 y prot-C^2 como sea necesario para apoyar la misión de la unidad. El producto del atq´- C^2 será una priorización de la lista de objetivos adversarios vulnerable y crítico como un trabajo inicial. Similarmente, los objetivos de la prot-C^2 deberían ser identificados en términos de criticabilidad y vulnerabilidad, luego priorizarlo.

80. CONCEPTO DE OPERACIONES (PASO 3)

a. El tercer paso del proceso de planeamiento de las OI es la formulación de un concepto de opns de OI para influir el C^2 adversario mientras protegemos el C^2 amigo. El C-3/G-3 revisa su juego de potenciales objetivos de atq´-C^2 y prot-C^2; evalúa las disponibilidades de OI para desarrollar el concepto de opns de OI que mejor apoye a la misión operacional total y que este sicronizado con el concepto de opn total.

b. La sincronización de las OI, tanto internamente (entre los cinco elementos de la G-C^2, los AC Y las RP) como externamente (a través de los SOC´s); es absolutamente crítico para alcanzar resultados decisivos en las dos disciplinas (atq´- C^2 y prot-C^2). El impacto de una sincronización apropiada será enfocar el efecto de todo el rango de posibilidades amigas para alcanzar el máximo efecto en el punto decisivo en tiempo y espacio.

c. Aunque la situación dictará las áreas críticas para la opn, el cmdte y el EM considerará en el planeamiento las áreas específicas sgtes:

(1) Los objetivos de las disciplinas de atq´-C^2 y prot-C^2 desde la perspectivas amiga y enemiga. El P/O u O/O básicos y el anexo de G-C^2, sincronizando la destrucción física, la GE, la SEGOPE, el engaño y las opns/sicolog para maximizar el atq´-C^2 y prot-C^2. Muchas actividades de G-C^2 pueden tener el efecto de maximizar la protección mientras degrada las capacidades de C^2 adversarias.

Otras influencias en el espacio de batalla del cmdte pueden impactar directamente sobre los éxitos de la misión.

(2) Las necesidades de IRI

(3) Las necesidades de apoyo de SINFOR

d. El EM considera todos estos factores para llegar a un concepto de opns de OI. Este concepto estará orientado al establecimiento del dominio de la info para dar a la fza dominante conciencia de espacio de batalla y control del AIM. Una herramienta crítica en el desarrollo de un efectivo concepto de opn, será la matriz de sincronización de OI; que está diseñada para acomodar los objetivos en tiempo-fase a lo largo de un eje horizontal contra el rendimiento de las unidades usualmente organizado por SOC a lo largo de un eje vertical. Dentro del cuadro de la matriz, se identifican las tareas críticas que deben realizarse para alcanzar los objetivos de OI, ayudando al planificador en el reconocimiento de interrelaciones entre tareas específicas y acciones, y la necesidad de orquestarlas de tal manera que se maximice su impacto en la ejecución. La Figura 15, muestras un ejemplo de matriz de sincronización de OI.

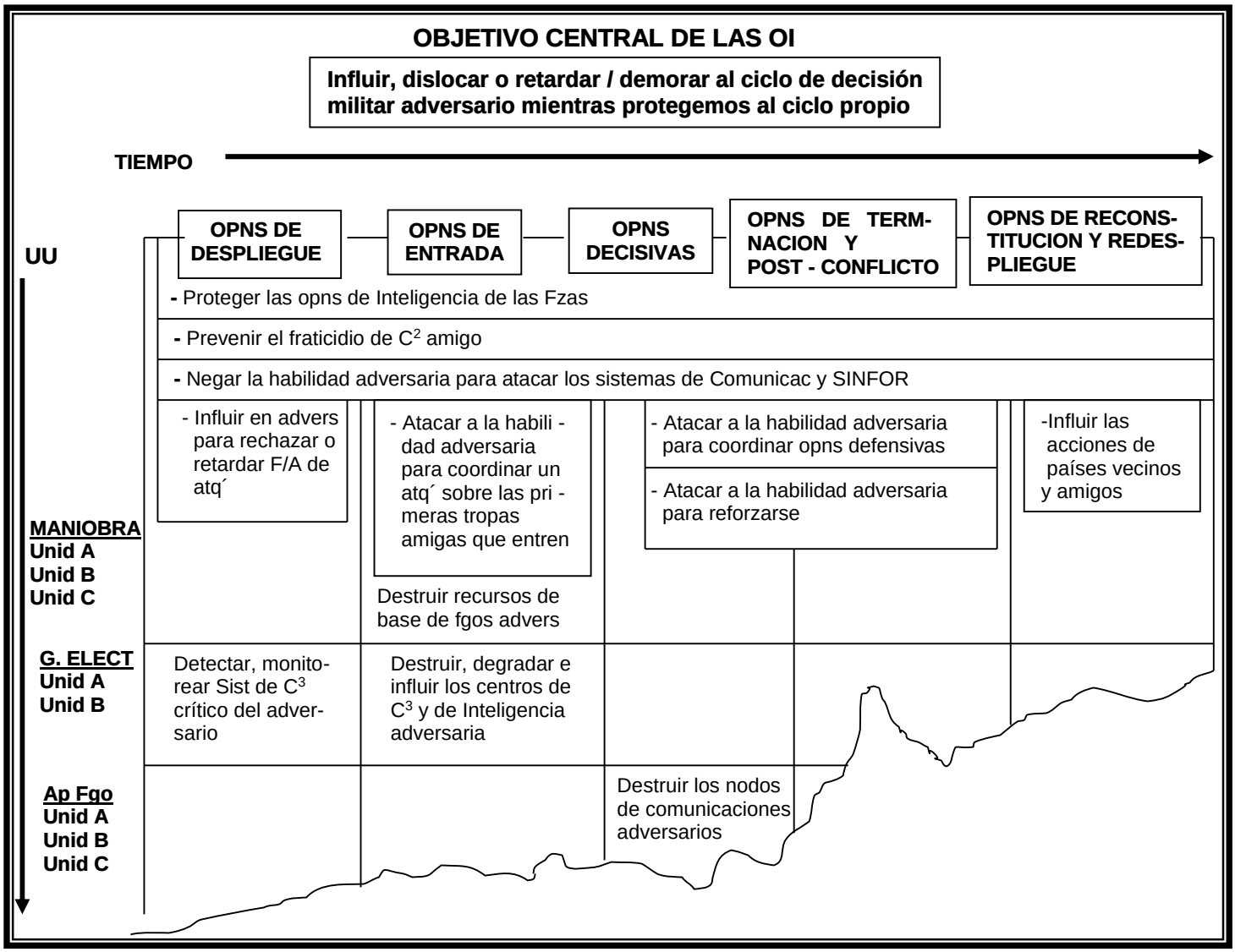

FIGURA 15: MATRIZ DE SINCRONIZACION DE OI

81. EJECUCION DE LAS OI (PASO4)

a. La ejecución empieza con la asignación de tareas a aquellos elementos que conducirán las misiones de OI. El C-3/G-3 controlará y dirigirá las fases de planeamiento y ejecución de las OI, con apoyo del C-2/G-2 y del C-6/G-6, así como de elementos especialistas en OI que estuvieran disponibles o asignados al EM. Las claves aquí son:
   (1) Seleccionar la mejor capacidad de atq´-C^2 para el mejor efecto (negar, influir, degradar, destruir).
   (2) Sincronizar la aplicación de los efectos para reforzar los cinco elementos de la G-C^2, y posibilidades de AC y RP (no permitir que estos entren en conflicto (ver figura 9)).

b. La asignación de tareas de OI normalmente llega a ser una parte de la orden básica en el párrafo 3 (concepto de opns y en las instrucciones de coordinación). Adicionalmente los detalles de las OI serán cubiertas en un anexo separado que consolide las OI/G-C^2 aplicables en una discusión operacional coherente. Cuando un anexo de G-C^2 sea escrito, debería incluir una matriz de sincronización que establezca líneas de tiempo, responsabilidades, secuencia de acciones y efectos deseados.

c. Conforme el planeamiento y la ejecución tome lugar, los planificadores deberían considerar un número de factores más allá de las estrictas capacidades de combate. Estos factores incluyen:
   (1) El costo de oportunidad de una acción.- Esto es, ¿cuál es el equilibrio entre atacar o destruir la capacidad adversaria ahora o explotarla para una ganancia futura? Por ejemplo, la destrucción de facilidades de C^2 claves puede dar a un cmdte operacional libertad de acción al negar al eno un C^2 efectivo de sus fzas; sin embargo, el costo de oportunidad de esa acción podría ser el negar a los sistemas de inteligencia de Telemática amigo una valiosa fuente de obtención de info sobre el oponente en un nivel estratégico. Similarmente, la destrucción de las redes de defensa aérea puede dar al cmdte táctico una superioridad aérea local, pero también puede eliminar los únicos medios que el cmdte operacional tiene para seguir o identificar formaciones enemigas.
   (2) Restricciones políticas y legales/Reglas de encuentro.- Para entender su impacto sobre el enlace entre los niveles de la guerra. Los planificadores de objetivos requieren conocer las reglas de encuentro (o cbte) así como las leyes y políticas de estado para el atq´ a ciertas personas, lugares o cosas - ¿Cómo tratará el cmdte con redes de computadoras comerciales, redes de telefonía local o redes de datos celulares, que pueden no sólo apoyar al esfuerzo militar sino también a la población civil, al comercio e industria?.

d. Los planificadores deben estar conscientes que la contra-OI adversaria pudiera ser lanzada contra no solo las fzas militares sino también contra la infraestructura civil del país. La mera amenaza de tales acciones puede generar efectos significativos reales y sicológicos. Por ejemplo un anuncio adversario afirmando que ha insertado un virus en la opn de computador de una institución bancaria, podría ocasionar pánico con mayores

repercusiones económicas, sin interesar la actual ejecución adversaria de tal ataque.

82. RETROALIMENTACION (PASO 5)

El quinto paso es el establecimiento de mecanismos de retroalimentación y monitoreo. Un proceso continuo de evaluación de daños o efectos será crítico para que el cmdte revise apreciación de situación y ajuste sus operaciones.

SECCIÓN IV. EJECUCION DE LAS OI

83. LA ESTRATEGIA MILITAR NACIONAL Y LAS OI

a. La realidad global de hoy está en un periodo de cambios significativos, las fuerzas armadas en general y el ejercito en particular deberán tener la habilidad para responder rápida y decisivamente a requerimientos que se podrían presentar en cualquier parte de nuestro territorio y eventualmente fuera de él. La situaciones de conflicto en el ámbito regional pueden presentarse, provocadas por amenazas dentro y fuera del país, que podrían obligar al empleo del ejército, el cual esta iniciando su proceso de modernización, pero también de reducción en el número de efectivos y cantidad de unidades, para hacerlas más técnicas y profesionales con equipamiento acorde al "estado de arte" y con posibilidades de poder desplegarse y actuar rápidamente con precisión y eficiencia.

b. Es también evidente que en eventuales conflictos o guerras, que el ejército deba actuar, deberá hacerlo en conjunto con otros institutos para alcanzar objetivos estratégicos. Todo esto, aunado a los avances en la tecnología de las armas, hacen que el C^2 sea crítico en la etapa de ejecución de las operaciones y que se deba desarrollar una nueva estrategia militar acorde a la realidad actual, con capacidad de enfrentar nuevos retos y amenazas. La G-I y la G-C^2 son parte de esta nueva estrategia que permitirá ejecutar las operaciones de info, en un ambiente tecnológico y dominado por la información que inunda todas las esferas o ámbitos no solo nacionales sino mundiales.

c. Se ha desarrollado un nuevo concepto estratégico para los ejércitos modernos, con la finalidad de demostrar habilidad para rápidamente entrar en alerta, movilizarse, desplegarse y operar , en cualquier lugar del propio territorio para defender los intereses nacionales y eventualmente proyectarse fuera de él para la seguridad de la nación. Está estrategia es de naturaleza conjunta, por lo que la sincronización del empleo de fuerzas terrestres, aéreas, marítimas y de operaciones especiales será crucial. Esta estrategia es conocida con el nombre de "proyección de la fuerza" y demandará un proceso de tecnificación de todos sus estamentos para una fuerza armada pequeña.

d. Está estrategia de proyección de la fuerza sigue una secuencia general de etapas que a menudo se superponen en tiempo y en espacio; donde las OI con sus consideraciones y acciones, podrán ser aplicadas enfocándose en el apoyo de info al comando de batalla durante las operaciones conjuntas contra el C^2 adversario. Estas etapas son operaciones que rara vez se inician con una idea clara de un "paquete entero" o propósito; muy por el contrario, se desarrollarán por "bits y piezas", con algunos arranques falsos

y subsiguientes ajustes mayores. Las acciones enemigas posteriores cambiarán "la ecuación", por lo que las operaciones de proyección de la fuerza sólo terminarán cuando la misión se halla completado y el último soldado retorne a su cuartel de origen.

e. Los Comandantes deberían asumir que no existe un juego arreglado de eventos, sino que deberían estar preparados para tratar con muchas actividades con sus correspondientes "mares de información", conceptualizando un flujo lógico a través de las etapas. En muchas situaciones las organizaciones del AIG estarán presentes en la zona de responsabilidad antes que las fuerzas lleguen; ellas estarán bien afianzadas con un marco logístico establecido y con enlaces y coordinaciones arregladas por su larga permanencia. Por ejemplo, inicialmente los medios de comunicación podrían conocer mejor la zona de responsabilidad que los militares, cubriéndola con reporteros, enviados especiales, corresponsales de guerra, etc; para obtener un entendimiento total y formar su propia perspectiva sobre la situación. Con los medios noticiosos nacionales e internacionales "observando" la llegada de fuerzas militares a su zona de responsabilidad, obliga a que personal de AC y de RP se desplieguen por adelantado para apoyar al Comandante y a la fuerza en sus interacciones con estas organizaciones, buscando no sólo reducir las distracciones potenciales al Comandante sino también educar a estas organizaciones y facilitar sus esfuerzos proporcionándoles información exacta, balanceada, creíble y oportuna para sus agencias y audiencias.

f. La infraestructura de comunicación de nuestras fuerzas debe ser capaz de proporcionar los medios para integrar las capacidades de C^4I empezando desde la instalación de la plataforma de proyección de la fuerza con posibilidades de alcance hacia atrás durante todas las etapas de las operaciones de proyección de la fuerza. La variedad de condiciones bajo las cuales el ejército será empleado en la era de información requerirá de una estrecha coordinación, integración y sincronización de las OI desde el nivel estratégico al nivel táctico.

g. Las etapas de las operaciones de proyección de la fuerza usualmente incluyen:
   (1) Movilización (si fuera necesario)
   (2) Operaciones de predespliegue
   (3) Operaciones de despliegue
   (4) Operaciones de entrada
   (5) Operaciones decisivas
   (6) Operaciones de postconflicto o postcrisis (culminación)
   (7) Operaciones de reconstitución y redespliegue (desmovilización)

   La figura 16, ilustra el ciclo de las operaciones de proyección de la fuerza.

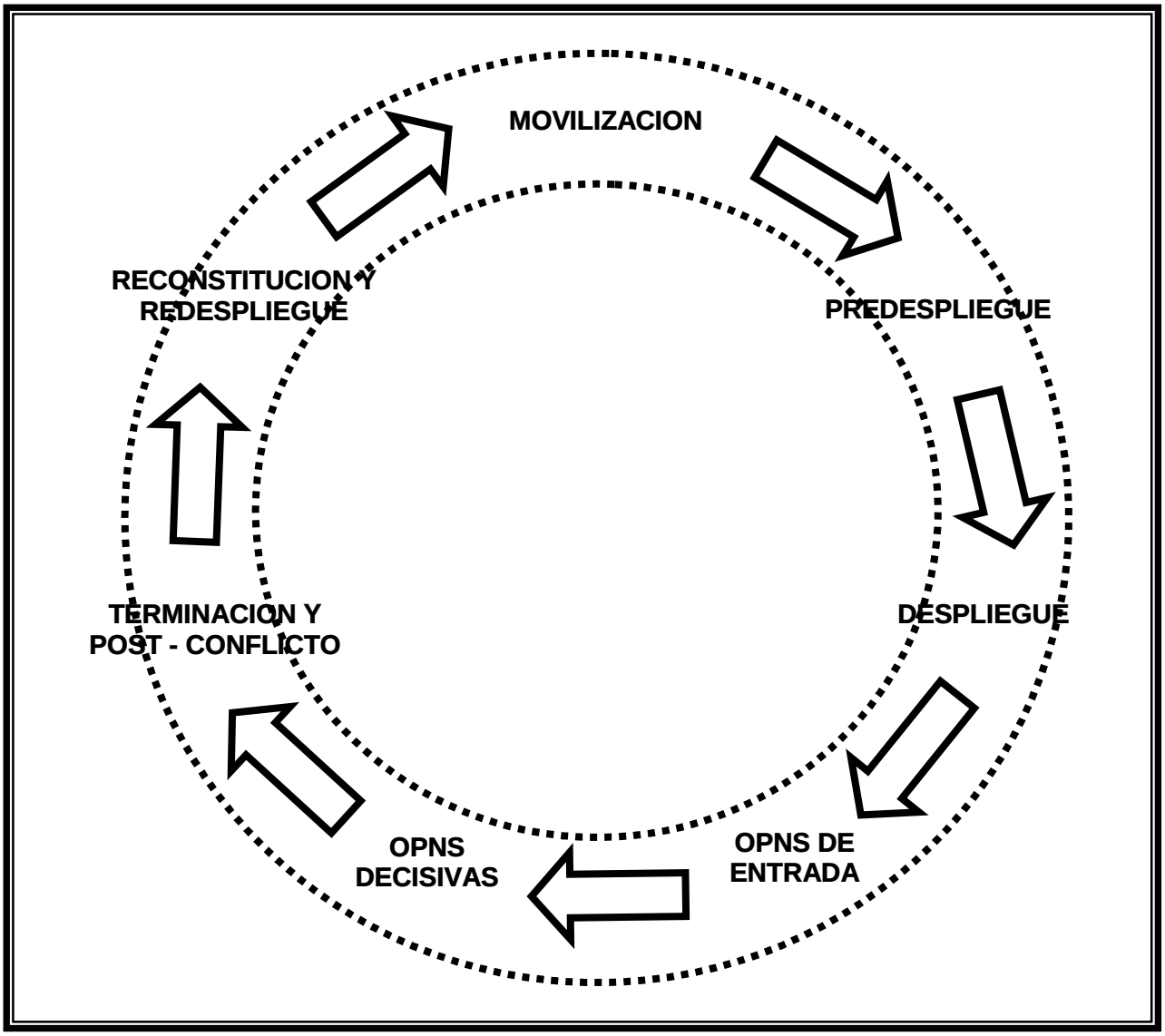

FIGURA 16: CICLO DE LAS OPNS DE PROYECCION DE LA FZA

84. OPERACIONES DE MOVILIZACION

a. La movilización es una operación intensiva de información. Una vez que se declara o decreta la movilización, las unidades deberán ejecutar una serie de actividades donde las OI podrán apoyarlas en la sincronización de la llegada, procesamiento, certificación y desplazamiento a los puntos finales, de los contigentes. El ejército dependerá de la administración de recursos de info provenientes de los comandos de movilización, que cuentan con sistemas que están sobre la infraestructura de info nacional (IIN) que emplean plataformas comerciales, tales como computadoras personales (PC's).

b. Las actividades de $G\text{-}C^2$ durante la movilización estarán predominantemente relacionadas con la protección de la info, las cuales deberán ser incluídas por el Cmdte en sus planes como medidas de protección de la disponibilidad, integridad y confidencialidad de info

clasificada o no, pero necesaria para apoyar a las operaciones de movilización.

c. Durante esta etapa de la proyección de la fuerza, los bits de información son transferidos en transmisiones de radio militares y públicas no seguras, en llamadas telefónicas, comunicados públicos, conversaciones, etc; que posibilitarán a los medios de comunicación personal u analista de inteligencia hostil juntar las piezas de la intenciones y capacidades nuestras. La SEGOPE y la SEGINFOR ayudarán al Cmdte para evitar que los adversarios obtengan y reúnan información de valor para la inteligencia de los bits de info que se transfieran.

85. OPERACIONES DE PREDESPLIEGUE

a. Los Cmdtes establecen objetivos y necesidades de la unidad para sentar la etapa para las actividades de predespliegue y buscar la preservación de los recursos de la fuerza y de sus posibilidades de toma de decisiones. Las OI integran los elementos de la G-C^2 para enmascarar el predespliegue y mejorar las operaciones de engaño. Los planes incluirán:
   (1) Enganche o combate a los SINFOR adversarios.
   (2) Identificación de tareas, establecimiento de objetivos de G-C^2, procedimientos específicos e instrucciones de coordinación; todas ilustradas, proyectadas o mostradas dentro de una matriz de sincronización de OI detallada.

b. Durante esta fase, los SINFOR tácticos continuarán empleándose menos que los sistemas civiles y militares fijos y sólo para acciones de rutina. Los sistemas militares que enlazan los escalones operacional y estratégico tales como la "Red de Sistemas de Información de Defensa (RSID)" y la "Red de Conmutación de defensa (RCD)", serán los principales sistemas militares dedicados que se usarán.

c. Las actividades de inteligencia continuarán girando alrededor de la base de datos adversaria que se estableció y de la PIC basada en la info. Los comandos necesitarán inteligencia nacional y datos sobre el clima, que los apoyen en el planeamiento detallado. Antes del despliegue, el EM debería desarrollar las NICC, NPI, las operaciones civiles - militares y los planes de R&V, inteligencia y adquisición de blancos.

d. Las acciones de G-C^2 continuarán concentrándose en la protección de la info a través del ejercicio de los procedimientos de SEGOPE. Con el apoyo del Cuartel General superior conjunto y el EAGIT, los planificadores de la G-C^2 consideran las acciones ofensivas para establecer el dominio de la info una vez que la fuerza empieza a desplegarse. Se necesitará una estrecha coordinación con personal de RP durante el planeamiento del engaño y de las opns/sicolog para mantener la SEGOPE y asegurar que tales esfuerzos no afectarán las audiencias propias o aliadas. Un programa de relaciones públicas (RP) sincronizado contribuirá a incrementar el entendimiento de las tropas, su confianza, dedicación, disciplina, deseo de vencer y confianza pública en el ejército.

86. OPERACIONES DE DESPLIEGUE

a. Las OI serán necesarias para establecer las condiciones de despliegue de fuerzas en una Z/O. Este despliegue requerirá de comunicaciones

conjuntas en tiempo casi real, estructurado para un rápido despliegue, apoyar en la ruta, y enlazar los niveles táctico y estratégico.

b. Durante esta etapa, las funciones de planeamiento de EM intensifican sus planes de contingencias y las NPI serán actualizadas, completadas o ajustadas. Los Cmdtes y planificadores de EM dan un toque al sistema de planeamiento conjunto y a sus base de datos para determinar la secuencia y disponibilidad de recursos. Conforme las fuerzas empiezan a desplegarse, los Cmdtes planean el impacto de su separación o sobre extensión y del apoyo de info reducida por el empleo de sistemas de baja capacidad, ajustando sus NICC para aquellas más críticas que mantengan la conciencia situacional, el nivel de entrenamiento y el cumplimiento de la misión.

c. Los SINFOR que se requerirán para el despliegue de las fuerzas demandarán comunicaciones seguras, flexibles y portátiles; con capacidad para interoperar con fuerzas conjuntas; y con enlaces múltiples y continuos de inteligencia y logísticos. Durante el despliegue, los escalones EO y superiores ejecutarán muchas de las acciones de G-C^2 tales como engaño, opns/sicolg y SEGOPE.

87. OPERACIONES DE ENTRADA

a. Las operaciones de info son necesarias para establecer las condiciones para entradas anticipadas. Las posibilidades de las OI son desplegadas en un área de contingencia para obtener info que necesita el Cmdte mientras niega al eno el uso de sus posibilidades de info y OI.

b. La defensa aérea es la clave para contrarrestar el R&V, inteligencia y adquisición de blancos (R&VIAB) adversario, durante el período de la entrada anticipada y donde nuestras fuerzas serán más vulnerables; ya que la entrada se realice con oposición o sin oposición del eno:

(1) **Entrada sin oposición**

Esta entrada permite un gran uso de las posibilidades de OI, enfocándose en apoyar a las fuerzas de avanzadas, confiando en el apoyo de comunicaciones y de inteligencia proveniente de los nodos militares de retaguardia y/o sistemas comerciales si están disponibles.

(2) **Entrada con oposición**

(a) En este caso, los Cmdtes pueden tener que confiar en un limitado número de SINFOR para obtener la info que necesitan para cumplir la misión; debido a esto las necesidades bien pueden sobrepasar la capacidad de los recursos disponibles, por lo tanto los Cmdtes deberán priorizar claramente sus necesidades de info para centrar mejor el empleo de estas limitadas capacidades.

(b) Trabajando dentro del plan de la G-I/G-C^2, los comandos del ejército emplearán sus capacidades de G-C^2 para cumplir sus tareas asignadas. El éxito de las operaciones de entrada con oposición puede mejorarse significativamente mediante la negación al adversario del uso de sus SINFOR a través del empleo de los recursos de ataq'-C^2, que podría incluir engaño o sobrecarga de los SINFOR adversarias y la dislocación o perturbación del empleo de su espectro electromagnético.

88. OPERACIONES DECISIVAS

a. Los Cmdtes visualizan al espacio de batalla y desarrollan conceptos operacionales que usan conciencia situacional común y la habilidad para mover info con rapidez y precisión sobre el campo de batalla. Las capacidades disponibles de OI de la unidad permitirán la sorpresa y la derrota decisiva del adversario desde posiciones dispersas, la cual usualmente se cumplirá de manera más efectiva contrarrestando las fortalezas enemigas con sistemas y métodos asimétricos o disímiles.

b. Las unidades empiezan conduciendo operaciones de G-C^2 ofensiva, que requerirá de los Cmdtes amigos ejercer un control superior sobre el ritmo de las actividades del campo de batalla. Los Cmdtes tácticos balancearán su superioridad de la info empleando sistemas de armas, incluyendo recursos conjuntos y regularán el ritmo y naturaleza de las acciones enemigas.

c. Para optimizar el flujo de info esencial, los Cmdtes priorizarán sus necesidades de info a través de las NICC y POV's. El EMBOI se asegurará que la G-C^2, los AC y las RP estén integradas en el concepto de operación del Cmdte. Esto se cumple conforme el G-3 integre sus recursos de OI en el esquema operacional para obtener el mejor marco posible basado en la intención del Cmdte. Más aún, el G-3 balancea organizaciones y recursos desde el AIG, esto son, recursos de inteligencia conjuntos y nacional, para completar el mosaico de PIC. A menudo, los recursos disponibles serán menores que aquellos que se necesitan para realizar las OI deseadas; por lo tanto el Cmdte proporcionará la priorización de los recursos. El monitoreo constante de la situación de la OI amiga y enemiga, asegurará que esta info sea incluida en la actualización de la situación, la PIC y en el CCR del Cmdte de su espacio de batalla.

d. La unidad de esfuerzo y la concentración de los efectos del poder de combate serán posibilitados por el mejoramiento del flujo de info, tanto vertical como horizontalmente entre Cmdtes y miembros de EM, apoyados por SINFOR militares. Las unidades tácticas emplearán la info militar para integrar totalmente los sistemas, posibilidades y funciones de los equipos de armas combinadas en la conducción de operaciones decisivas. El control descentralizado de maniobras y encuentros es alcanzado mediante la optimización de la conciencia situacional y las comunicaciones proporcionadas por conectividad digital. Esta habilidad permite a las unidades tácticas la oportunidad de evitar las fortalezas del adversario y la detección de medios mientras se mueven hacia posiciones más ventajosas para permitir la destrucción de la fuerza ena tanto en operaciones ofensivas como defensivas. Las unidades ejercen la capacidad de enfocar y concentrar los efectos de los fuegos indirectos contra el adversario y sincronizar sus efectos con la maniobra. Mediante el empleo de la artillería altamente maniobrable, plataformas de aviación, sensores digitales y sistemas de campos minados inteligentes; las unidades de maniobra podrán establecer enlaces de fuego-rápido sensor-lanzador.

e. La conciencia situacional mejorada y las posibilidades de comunicaciones permitirán al Cmdte de maniobra conducir golpes decisivos dentro de la profundidad ena mediante el empleo de sistemas de fuego orgánicos y de

apoyo. Los Cmdtes usan el atq'-C^2 para destruir, dislocar y explotar los SINFOR eno, Proporcionando un CCR a todas los escalones las OI facilitan la sincronización de toda la potencia combativa a través de los SOC's. En conjunción con los planes de batalla terrestres y aéreos, los Cmdtes deben seleccionar los nodos vulnerables y saber si se le destruirá o se le perturbará y cuando explotarlos a través de la G-C^2.

89. OPERACIONES DE CULMINACION Y POST-CONFLICTO

a. Después del conflicto, es posible que se deje una dislocación significativa de la infraestructura y la población en el área de conflicto. En estas circunstancias la protección de la info por la SEGOPE, la cesión de info militar a otras organizaciones no militares y aún la continuación de la reunión de nueva info puede llegar a ser necesario. Cierta info militar será protegida, mientras otras serán entregadas para que sean hechas públicas para prevenir que más adelante no existan motivos o excusas para nuevos brotes de tensión o muertes inútiles y para permitir que se reasuma las actividades normales. Por ejemplo el revelar las zonas de campos minados.
b. Las dislocaciones y daños que siguen a un combate generan necesidades de nueva información. Monitorear, reubicar y proporcionar asistencia o apoyo humanitario para los desplazados es tanto un problema de info como logístico. Igualmente la destrucción de infraestructura logística, puede obligar a dejar cierto equipamiento militar en operaciones, como por ejemplo puentes temporales que reemplacen los destruidos, equipos de trasmisión de bandas de radiodifusión, generadores eléctricos, purificadores de agua, etc. La info será crítica para tomar estas decisiones.
c. Cuando las operaciones de combate provocan el final del conflicto, habrá un periodo de transición hacia las operaciones de post-conflicto, que puede ocurrir aún cuando se estén librando combates aislados en algunas partes de la Z/O. Por eso, los ajustes a las OI deben anticiparse y planearse para asegurar una transición suave durante los periodos críticos después que se detiene la lucha, enfocándose en proporcionar apoyo para la preparación del redespliegue de las fuerzas y continuar su presencia para permitir a otros elementos del poder nacional alcanzar sus metas estratégicas.

90. OPERACIONES DE REDESPLIEGUE Y RECONSTITUCION

a. Normalmente, las acciones de reconstitución y redespliegue ocurren en un ambiente benigno, aunque no siempre será así. La sensitividad a los efectos que la info tiene sobre la población será una consideración.
b. En esta etapa, las OI apoyan al redespliegue de los recursos no más de lo necesario, continuando el énfasis en la SEGINFOR durante las operaciones de redespliegue.

ANEXO 01: PLANES Y ORDENES DE OI Y G-C^2

01. ASPECTOS INTRODUCTORIOS

a. Este anexo ilustra y explica como podrían incorporarse las OI y la G-C^2 en un plan u orden básico. El mismo formato de cinco párrafos ampliamente conocido, se emplea para la explicación.

b. Los planes y ordenes trasladan info e instrucciones a las unidades subordinadas y emplean formatos similares. Aunque un plan puede entrar en vigencia de manera inmediata para propósitos de planeamiento o para una acción preparatoria específica, éste no será ejecutada hasta que el Cmdte que lo emitió lo disponga, que usualmente será cuando ciertas condiciones específicas prescritas en el plan se cumplan. Un plan siempre deberá especificar el tiempo o condiciones bajo las cuales será efectivo. Un plan llega a ser una orden cuando se disponga su ejecución.

02. EJEMPLO DE UN MODELO DE PLAN DE OI DE NIVEL OPERACIONAL

A continuación se presenta un modelo de plan de OI de nivel operacional, al cual también se le puede denominar Plan de OI para Opns mayores o simplemente Plan de Campaña para OI.

COPIA Nº ..... de ..... COPIAS
Cuartel General emisor

Lugar de emisión
GFH

PLAN DE OPERACION MAYOR (NOMBRE O NOMBRE)
Referencias: Cartas, mapas y otros documentos
Organización de Tarea/Relaciones de Comando
(Ver Anexo 01, Organización de tarea)

1. **SITUACION**.- Integrar las consideraciones tácticas importantes para las OI en las fases iniciales de una opn dentro de la descripción total de la situación operacional. Hacer referencia a las apreciaciones de Cmdo y EM, estudio del país de interés u PP/OO. Indicar eventos desencadenantes que podrían señalar la ejecución de componentes específicos para una OI dentro de la O/O
   a. Fuerzas enas.- Integrar las amenazas adversarias a las OI amigas. (Ver anexo 02, Inteligencia)
   b. Fuerzas amigas.- Proporcionar info sobre fuerzas amigas que pueden afectar la ejecución de las OI. Estos efectos pueden directamente impactar sobre el comando o sobre las organizaciones subordinadas al cmdo.
   c. Refuerzos y unidades asignada a otros cmdos
   d. Suposiciones.- Integrar un resumen de las condiciones y situaciones que deben existir para mejorar las OI
2. **MISION**.- Direccionar las OI al grado necesario para completar el estado de toda la misión operacional.
3. **EJECUCION**

a. **Intención del Cmdte.- Incluir brevemente como las OI apoyarán la misión dentro del contexto de la visión total de la opns del Cmdte**.

b. Concepto de opns.- Incluir una expresión clara y concisa de las tareas esenciales de las OI que se cumplirán en todas las fases de la opns mayor. Un ejemplo es la legitimación de toda la campaña a través de las OI preparando a la gente en la zona hostil para aceptar los resultados de la opn, especialmente si la derrota pudiera ser vista con resentimiento. Resumir las tareas de OI Asignadas por el Cmdo y otras tareas informacionales derivadas del análisis del ambiente del cmdte y su entendimiento de las intenciones superiores. En el nivel operacional, el concepto de opn usualmente está dividido en fases.

(1) PRIMERA FASE.- La primera fase operacional de una contingencia usualmente es la preparación del cmdo para ejecutar la opn. Los elementos OI que a menudo se emplean en esta fase incluyen lo sgte:

(a) Establecimiento del enlace con varias dependencias; incluyendo al cmdo unificado responsable por el área objetivo, con otros cmdos unificados o subunificados (especialmente aquellos involucrados en el despliegue), con fuerzas de opns especiales en el área objetivo y con dependencias apropiadas del estado. Cada uno de estos enlaces formarán una porción del apoyo total de las OI.

(b) Empleo del apoyo diplomático y dependencias legales para asesoramiento en acuerdos, restricciones, reglas de compromiso, en coordinación con asesor legal.

(c) Establecimiento de SINFOR adelantados para establecer C^2 y para asesorar en el establecimiento o preparación de zonas o áreas intermedias en el área objetivo y dirigir la reposición de abastos y equipos.

(d) Empleo de AC, RP y Opns/Sicolog para apoyar iniciativas políticas y diplomáticas.

(e) Trasmisión de la intención del cmdte y esquema de maniobra operacional, incluyendo la batalla estrecha, batalla en profundidad y opns de seguridad en la retaguardia para asegurar un entendimiento y ejecución simultanea de opns complejas por todos los participantes.

(f) Apoyo de fuegos operacionales con OI tales como GE, y apropiados arquitecturas de C^4I

(g) Determinación de OI para apoyar AC, defensa aérea, GE, opns/sicolog, opns de retaguardia, protección de las fzas y medios, funciones de la PM y RP

(h) Desarrollo de secuelas y ramificaciones de OI.

(i) Proporcionar instrucciones de coordinación aplicable a 2 o más elementos subordinados que ejecutan OI.

(2) SEGUNDA FASE.- La segunda fase operacional es usualmente la ejecución de la opn en si misma y direcciona aquellos aspectos de las OI que juegan un rol importante en apoyo a esta fase. Comprende:

(a) Incluir en la descripción del concepto de opns, el rol de los elementos de OI en el mejoramiento de la efectividad de las unidades mayores.
(b) Presentar el esquema de maniobra, así como el esquema de despliegue, de las unidades de OI para alcanzar los objetivos iniciales. El esquema debería incluir, donde sea apropiado, la inserción forzosa de elementos de combate y si fuera necesario elementos de C^2 y su apoyo que lo acompaña. Considerar lo sgte:
1.- Secuencia de unidades informacionales conforme la situación operacional llegue a ser más clara. El despliegue de elementos informacionales puede ser acelerado o retardado como sea apropiado.
2.- Cambios en la naturaleza de la opn.
3.- Mayor reagrupamiento de fzas informacionales.
4.- Cambios significativos en las capacidades enemigas que podrían afectar a las unidades informacionales necesarias en la opn.
(c) En el subpárrafo de apoyo de fuegos o en su anexo, direccionar las interfaces conjuntas y las consideraciones de OI que guían tales interfaces.
(d) Incluir provisiones de OI para AC, defensa aérea, GE, opns/sicolog, opns de retaguardia, protección de fzas y medios, funciones de PM y RP.
(e) Como sea necesario, establecer la ubicación y tareas para los elementos de OI que se mantienen en reserva.
(f) Incluir instrucciones de coordinación que se aplican a dos o más elementos subordinados que ejecutarán las OI. Incluir también procedimientos de enlace a través de las OI entre la fza y fzas que ya están en la opn, si fuera apropiado.

(3) TERCERA FASE.- La tercera fase operacional es usualmente la consolidación de los resultados de un estado final exitoso para esta fase. No contiene el detalle que se incluye en la fases precedentes, sino que el apoyo será direccionado como sea apropiado.

c. Tareas para los Comando mayores subordinados.—Asegurarse que las OI están direccionadas apropiadamente para cada cmdo mayor subordinado.

d. Instrucciones de coordinación.- Integrar las instrucciones sobre G-C^2 siempre que sean afectadas dos o más fases de la opns. Las instrucciones de coordinación pueden incluir:
(1) Tiempos, eventos o situaciones que puedan señalar la transición de varios OI entre fases.
(2) Restricciones y/o limitaciones.
(3) Reglas de compromiso, sobre todo aquellas referidas al empleo del espectro electromagnético, redes de computadoras e interferencia de comunicaciones y otras Telemática.
(4) Guía para la administración de recursos que pueden limitar las OI (por ejemplo, limitados circuitos de comunicaciones, limitado acceso a redes, etc).

(5) Orientación sobre el entrenamiento concerniente a procedimientos de OI.
(6) Orientación para el planeamiento operacional que involucre OI.
(7) Opns de relaciones públicas.

4. **ADMINISTRACION**.- Insertar info específica de como las OI apoyan a los elementos del ejercito envueltos en una opn. En este párrafo o en su anexo los cmdtes de lo Cuarteles Generales incluyen OI entre descripciones de aquellos asuntos de apoyo necesario para cumplir la misión de cbte de su fza.
5. **COMANDO Y TELEMÁTICA**
   a. Comando.- Colocar las necesidades de enlace y designar PC alternos y la línea o sucesión de comando, si no estuviera en el POV. Incluir también ubicaciones de PPCC y el eje de desplazamiento del PC si no estuviera mostrado sobre un calco que acompañe el plan.
   b. Telemática.- Como mínimo, indicar el índice de la IOCE. Las instrucciones en este subpárrafo pueden hacer referencia a un anexo, pero al menos debería incluir reglas concernientes al uso de comunicaciones y otros equipos electrónicas (por ejemplo, radio silencio).

ANEXOS: Reconociendo la expansiva contribución que las OI pueden hacer al cumplimiento de la misión en su conjunto, los anexos del P/O han sido reorganizados para crear un nuevo anexo de G-C^2, que consolide los tradicionales anexos que traten con el engaño, la GE y las opns/sicolog.

ANEXO 01: **ORGANIZACION DE TAREA/RELACIONES DE COMANDO**.- Para un plan de una opn mayor compuesta de algunas fases, este anexo identifica e integra la organización de tarea que se requiere para conducir OI. Recalcar las relaciones de cmdo y sus cambios, si hubieran, conforme las OI progresan de una fase a la siguiente. Relacionar la estructura informacional contra las interfaces esperadas y con las actividades envueltas en la opn sgtes:

1. Relaciones civiles-políticas.- consulados, agencias internacionales, etc.
2. Relaciones conjuntas.- Ministerio de Defensa, CCFA, Secretaria de defensa, otros institutos armados, PNP.
3. Otras fzas del ejército.- La estructura informacional que posibilita la conectividad desde el nivel más alto del componente del ejército que participa en las opns hasta el más bajo, incluyendo:
   a. Componentes del ejército de cmdos subunificados y fzas de tarea conjunta.
   b. Cmdos funcionales
   c. Cmdos de área.

d. Organizaciones mayores de cbte y apy de cbte bajo el mando del C-TO.
e. Cuarteles Generales, especialmente desplegados para estructuras informacionales, tales como unidades de comunicaciones.

ANEXO 02: **INTELIGENCIA**.- Este anexo debería incorporar información crítica necesaria para apoyar las OI e integrar estos elementos dentro de una gran misión de la situación ena.

ANEXO 03: **CALCO DE OPERACIONES**.- Representación gráfica del concepto de opns.

ANEXO 04: **G-C^2**.- Este anexo se enfoca en proporcionar la info necesaria para conducir opns de G-C^2 para identificar y sincronizar mejor la aplicación de las capacidades disponibles para cumplir la misión total.

ANEXO 05: **RESTRICCIONES**.- Este anexo contiene aquellas limitaciones políticas, humanitarias, económicas y sociales/culturales sobre la aplicación del poder militar durante la opn.

ANEXO 06: **REGLAS DE COMPROMISO**.- Contiene orientaciones para las organizaciones subordinados y de apoyo relacionadas a las reglas para el control de fzas y sus sistemas de armas, incluyendo guías para la conducción de OI.

ANEXO 07: **APOYO DE FUEGOS**

ANEXO 08: **DEFENSA AEREA**

ANEXO 09: **INGENIERIA**.- Debería incluir una expresión de cómo se levará a cabo el apoyo de ingeniería, incluyendo prioridades de tareas de movilidad, contramovilidad y supervivencia dentro de sectores y prioridad de recursos de ingeniería para unidades o sectores subordinados.

ANEXO 10: **COMUNICACIONES-ELECTRONICA**.- Este anexo describe el enlace proporcionando por el ctel gral de la fza entre el sistema de C^2 táctico del ejército, que existe entre sus unidades subordinados; y los sistemas de C^2 conjunto. Se mencionan SINFOR que deberán estar cuidadosamente coordinar con las opns de G-C^2.

ANEXO 11: **OPNS DE RETAGUARDIA**.- Este anexo contiene una guía y prioridades para la seguridad de instalaciones y áreas de retaguardia para prevenir o minimizar, o el movimiento de tropas amigas. Se designa a una unidad para encontrar, fijar y destruir las incursiones enas en el área de retaguardia y provee un área de control de daño después de un ataq' o incidente.

ANEXO 12: **PROTECCION**.- Este anexo contiene instrucciones para la protección de bases, instalaciones, personal militar, miembros familiares u otros nacionales en el TO, contra el terrorismo, desastres naturales y otros peligros. Contiene también info sobre la protección de la arquitectura de C^4I

ANEXO 13: **OPNS DE POLICIA MILITAR**.- Este anexo incluye las misiones de la PM sgte: seguridad del área, control de circulación del campo de batalla, opns de prisioneros de guerra y ley y orden.

ANEXO 14: **RELACIONES PUBLICAS**.- Este anexo contiene una guía para facilitar el esfuerzo de los medios por cubrir la opn y para apoyar las necesidades de info de las tropas y sus familias.

ANEXO 15: **ENTRENAMIENTO**

ANEXO 16: **ASUNTOS CIVILES**

03. EJEMPLO DE ANEXO DE G-C^2

COPIA Nº ..... de ..... COPIAS
Cuartel General emisor
Lugar de emisión
GFH

ANEXO 04 (GUERRA DE CONADO Y CONTROL) A LA O/O XX
Referencias:

1. **SITUACION**.- Describir totalmente el ambiente operacional aplicado a las OI, así como los aspectos apropiados al ambiente estratégico que pueden impactar a las OI. Incluir consideraciones tácticas importantes a las OI en las fases iniciales de una opn y establecer la más probable F/A de atq'-C^2 adversario. Indicar los eventos desencadenantes que podrían señalar la ejecución de componentes específicos de las OI dentro de la O/O.
   a. Fzas enas.- Expandir la discusión de la situación ena en términos de G-C^2, para incluir fortalezas y debilidades. Los componentes de info que se deberían incluir son:
      (1) Un resumen de info concerniente a la Z/O, consistente de:
         (a) Una visión estratégica del área que incluye como los factores del clima, los políticas, la geografía, la topografía, la demografía, la economía y lo socio-cultural; pueden afectar a las OI.
         (b) Específicar la info focalizada, particularmente las condiciones que afectan las primeras fases de la opn. Incluye la disponibilidad de tecnologías de avanzada dentro del área o zona tales como redes de info comerciales, nacionales o multinacionales (telefónicas, televisivas, enlaces satelitales y de administración de frecuencias) y el valor de su protección o alteración/perturbación.

      (2) Una descripción del adversario, consistente de:
         (a) Factores estratégicos y operacionales, tales como el nivel de sofisticación del uso de la tecnología de info por parte del adversario para difundir info contrarrestando esfuerzos nacionales contra su gente. Habilidad del adversario para establecer facilidades e instalaciones de info claves que hallan sido interrumpidas, y para mantener la iniciativa en la arena informacional. Experiencia pasada del adversario para tratar

con interrupciones y/o perturbaciones de sus SINFOR por largos periodos de tiempo (tales como los causados por desastres naturales, disensiones internas o fallas de subsistemas por perdidas de energía eléctrica); almacenamiento de componentes claves y vulnerabilidad a la dislocación o perturbación de la cadena de abastecimiento de equipos de info provenientes del exterior del país o Z/O.

(b) Factores de inmediato interés a las primeras fases de la opn concernientes a la existencia de técnicos y reparadores calificados en equipos de comunicaciones y de información.

(c) Orden de batalla de info, cantidad de SINFOR, personalidades líderes y nivel de entrenamiento o experiencia de combate.

b. Fzas amigas.- Establecer la misión y partes aplicables del concepto de opn a las OI/G-I de un cmdo conjunto del cual se es subordinado. Estos aspectos están normalmente escritos en el plan de campaña del TO. Proporcionar suficiente detalle para que los individuos claves conozcan y entiendan la intención del cmdte del elón sup conjunto, así como su estado final deseado a la conclusión de la campaña y como sus acciones engranan con los objetivos intentados.

(1) Cuartel general superior.- Incluir la misión, concepto de opn e intención del cmdte conjunto y/o unificado. Su concepto determina las contribuciones de varios elementos informacionales y desde los cuales muy probablemente se provean los apoyos.

(2) Otros componentes.- Destacar los roles de la fuerza aérea y la naval, en las OI/G-1.

(3) Fzas de opns especiales.- Si esta asignadas como reservas estratégicas.

(4) Otras dependencias del estado de interés para la G-C^2.

c. Unidades agregadas o a disposición de otros comandos.

d. Suposiciones.- se pueden incluir predicciones y presunciones concernientes a:

(1) Condiciones de la info dentro de la Z/O y países o región involucrada.

(2) Políticas nacionales previas que afectarán la velocidad y habilidad para cambiar temas informacionales.

(3) Involucramiento de potencias dentro o fuera de la región o zona de conflicto que podrían afectar las OI.

(4) Apoyos de agencias o dependencias internacionales que se relacionen a las OI.

(5) Consenso del grado o extensión de las OI que se conducirán en la Z/O.

(6) Disponibilidad de recursos informacionales.

(7) Tiempos y ubicaciones de acciones hostiles anticipadas conforme ellas afectan a las OI.

(8) El cronograma de empleo de eventos especiales en las OI.

2. **MISION**.- Incluir una expresión explícita de la misión de G-C^2 para apoyar la opn, tal como el ejemplo siguiente: "Con orden, el EO-SEL conducirá operaciones de G-C^2 para disuadir que AZUL ataque a ROJO. Si la disuasión falla, el día D a la hora H el EO-SEL conducirá operaciones de G-

C^2 para apoyar a las operaciones de combate para dislocar, desorganizar y/o interrumpir el C^2 de las fuerzas operacionales de AZUL y degradar la conciencia situacional de sus operaciones, mientras protegemos las posibilidades de C^2 propias contra los intentos de destrucción y desorganización o dislocación enemiga".

3. EJECUCION

a. Concepto de operaciones.- Proporcionar una discusión detallada de la operación de G-C^2 total, con los detalles específicos desarrollados en apéndices organizados alrededor de los cinco elementos de la G-C^2:

(1) Engaño militar.- En este subpárrafo o en su apéndice, incluir una descripción del objetivo de engaño, la historia de engaño, los recursos disponibles, selección de planes de engaño del elón sup; y, las medidas de engaño activas y pasivas que deben tomar las organizaciones subordinadas.

(2) Guerra Electrónica.- En este subpárrafo o en su apéndice incluir la misión de GE, las posibilidades de GE enemigas, las medidas de GE ofensivas y defensivas y la coordinación con otras partes del P/O (engaño, comunicaciones, opn/sicolog y fuegos)

(3) Seguridad de las operaciones (SEGOPE).- En este subpárrafo o en el apéndice indicar las medidas para negar información al enemigo concerniente a la velocidad y tamaño de la fuerza, así como la forma de acción específica que ejecutará el país en la fase de combate decisiva. Enfatizar en las etapas iniciales sobre la negación del acceso enemigo a sus propias capacidades de inteligencia y de ser posible a fuentes extranjeras. El engaño, las opns/sicolog, la GE y la destrucción física apoyarán estos objetivos.

(4) Operaciones sicológicas.- En este subpárrafo o en el apéndice hacer referencia al anexo inteligencia, designando objetivos de opns/sicolog y describiendo el plan de opns/sicolog para integrarlo en el plan del elón sup y cualquier plan de opns de engaño a tareas relativas para las unidades subordinadas.

(5) Destrucción física.- Cuando es empleada en el rol de G-C^2, la destrucción física será usada para destruir los sistemas de defensa aérea y de comunicaciones enemiga, sus capacidades de fusión y reunión de inteligencia y para destruir la habilidad ena para golpear las capacidades de G-C^2 y C^2 amigo.

b. Tareas de G-C^2.- Tanto impuestos como deducidos por el comando.

(1) Cuarteles generales mayores

(a) Ejercer la autoridad de coordinación centralizada de todas las operaciones de G-C^2 del TO.

(b) Asegurar que las responsabilidades de los elementos de EM para G-C^2 sean cumplidas de acuerdo a normas y disposiciones prescritas.

(c) Asesorar a los cmdtes del componente ejército y de apoyo del EO para sus objetivos de G-C^2 y proporcionar guía paras su cumplimiento.

(d) Desarrollar una lista de frecuencias restringidas conjuntas para apoyar las opns.

(e) Proporcionar supervisión y asegurar la coordinación de cualquier acción de reprogramación.

(2) Comandos componentes y de apoyo

(a) Proporcionar punto de contacto para G-C^2.

(b) Planear y estar preparado para conducir opns de G-C^2.

(c) Identificar cualquier opn que pueda impactar o degradar el C^2 efectivo de las fzas.

(d) Recomendar las necesidades de reunión de inteligencia del EO en apoyo a las opns de G-C^2.

(e) Dirigir la reprogramación de acciones como sea requerido.

c. Instrucciones de coordinación

(1) El elemento de planeamiento de EM de la OI del EO coordinará como sea apropiado, las acciones asociadas con opns contra el C^2 de AZUL. Estas acciones incluyen destrucción física, GE, Opns/sicolog, engaño y SEGOPE

(2) Planear y apoyar las opns de G-C^2 del EO, coordinando:

(a) Con otros institutos armados.

(b) Cmdos de opns especiales.

(c) Dependencias de inteligencia del estado de defensa e institutos.

(d) EAGIT.

4. ADMINISTRACION

Durante estas opns, la falta de estructuras de apoyo específicamente estandarizadas en fuerzas armadas y aún dentro del ejército, puede ser superada a través de una conectividad de información mejorada que este disponible en las bases de datos común y hardware y software común, o con equipos de enlace.

a. Las características de tales mecanismos podrían reducir el número de soldados o unidades expuestas a un ambiente operacional, con una alta relación de tropas de cbte para apoyar tropas en ubicaciones operacionales. Considerar algunas de las áreas sgtes para este tipo de idea:

(1) Informes sobre los efectivos de personal enviados electrónicamente.

(2) El apoyo de telemedicina reducirá la cantidad de especialistas desplegados en un área operacional.

(3) Situación de estaciones y estudios radiales y televisivos localizados fuera del área operacional inmediata que podrían usar o facilitar las opns/sicolog.

(4) Producción de diarios locales que podrían facilitar las opns/sicolog al mismo tiempo que se reduce el apoyo de infraestructuras dentro de una Z/O.

b. Identificar apoyo de redes de información de terceros países y establecer detalles de los procedimientos para hacer uso de estos recursos.

5. COMANDO Y TELEMÁTICA

Se puede hacer referencia al anexo respectivo.

APENDICES:

Apéndice “A”: Engaño Militar
Apéndice “B”: Guerra Electrónica
Apéndice “C”: Seguridad de las operaciones
Apéndice “D”: Operaciones sicológicas.

ANEXO 02 : RESPONSABILIDADES DE ORGANIZACIONES ESPECIALES DE G - C^2

01. CENTRO CONJUNTO DE G - C^2 (CC/G-C^2)

a. El CCFA debería ser responsable por crear, organizar y conducir el funcionamiento de uno o más CC/G-C^2 para proporcionar apoyo a fuerzas estratégicas con opns de G-C^2

b. La misión de este CC/G-C^2 será proporcionar apoyo directo a los Cmdtes operacionales con opns de G-C^2, integrando elementos constituidos de G-C^2, SEGOPE, opns/sicolog, engaño militar y destrucción física. Apoyará también aplicaciones militares de no-combate de G-I mediante el planeamiento y ejecución de las fases de las opns. Este apoyo será proporcionado en el orden de prioridad siguiente:
   (1) Cmdtes de fuerza conjunta (Cmdtes combatientes, Cmdtes unificados subordinados y Cmdtes de fza de tarea conjunta).
   (2) Cmdtes de componentes de instituto (terrestre, aéreo, marítimo)
   (3) Cmdtes de componentes funcional

c. El CC/G-C^2 también proporcionará apoyo al Ministerio de Defensa, Secretaría de Defensa Nacional y otras dependencias de ese nivel con autorización presidencial.

d. Funciones.- El CC/F-C^2, a través del director de la 3ra DIEMFA tendrá las funciones siguientes:
   (1) Interfacear con los otros directores, institutos, MINDEF y organismos del sector defensa y fuera de él, para integrar la G-I con los esfuerzos de G-C^2.
   (2) Analizar las posibilidades del sistema técnico operativo conjunto para optimizar el apoyo a las opns técnicas especiales para los Cmdtes combatientes.
   (3) Servir como un punto de contacto central de EM conjunto para revisar las misiones conjuntas de G-C^2.
   (4) Coordinar con el director de la 5ta DIEMFA para sistemas C^4 para recursos de prot-C^2.
   (5) Asesorar en el desarrollo de doctrina conjunta y de TTP's conjuntos para G-C^2 y GE.
   (6) Evaluar la efectividad en combate de la G-C^2.
   (7) Servir como punto focal del sector defensa para definir, coordinar y supervisar la integración de aquellas bases de datos y sistemas de datos, necesarios para establecer una base común de info conjunta para conducir G-C^2. Esta base de info consolida los sistemas de datos y bases de datos operacional e inteligencia (equipo, sistemas y fzas), incluyendo otros tipos de base de datos necesarios para conducir G-C^2 en el espacio de batalla de Cmdte combatiente.
   (8) Organiza, administra y ejercita los aspectos comunes de GE reprogramándolos si fuera necesario. Desarrollo procedimientos para asesorar a los Cmdtes con la identificación, validación y difusión de cambios en las amenazas electrónicas.

(9) Organizar y facilita el desarrollo de simulaciones de G-C^2 conjunta apoyando la materialización de juegos de guerra entre EEMM conjunto, institutos, Cmdo combatientes y otros del mismo nivel.
(10) Participa en la investigación y estudios de G-C^2 de naturaleza operacional para el MINDEF.
(11) Mantiene un conocimiento y coordina con los institutos sobre la ingeniería, iniciativas, programas y desarrollo de sistemas de G-C^2.
(12) Realiza análisis de vulnerabilidad y efectividad de equipos empleados en G-C^2, en coordinación con el director de la 5ta DIEMFA.

e. Equipos de A/D de G-C^2.- Para un apy directo de un Cmdte combatiente el CC/G-C^2 mantiene equipos desplegables de G-C^2 a pedido, para proporcionar análisis y asesoramiento oportuno para el planeamiento y coordinación de la G-C^2.

02. ELEMENTO DE ACTIVIDAD DE GUERRA DE LA INFO TERRESTRE (EAGIT)

a. La misión del EAGIT será coordinar la inteligencia multidisciplinaria y otros apoyos para el planeamiento y ejecución de opns, incluyendo apoyo de base de datos de G-C^2, inteligencia humana (INTHUMA), contrainteligencia (CI) e inteligencia técnica (INTEC). El EAGIT estará electrónicamente conectado con otros centros o facilidades de G-I de los institutos, de fuerzas conjuntas, del MINDEF y nacionales.
b. El EAGIT deberá ser específicamente diseñado para proveer apoyo estructurado a comandos componentes terrestres, con expertos técnicos que no cuentan los EEMM de dichos cmdos, para facilitar el planeamiento y ejecución de las OI/G-C^2. Este apoyo será con equipos de apoyo de campaña.
c. Estos equipos de apoyo de campaña se despliegan para asesorar y apoyar al Cmdte del componente terrestre en:
   (1) Protección de C^2 que incluye en:
      (a) Apoyo de seguridad de C^4
      (b) Análisis, investigaciones y vigilancias a evaluaciones de vulnerabilidades del C^2 de Cmdte del componente terrestre, al sabotaje, engaño y atq' de OI/G-C^2; y para evaluar su habilidad para mantener programas de seguridad y de protección de tales facilidades.
      (c) Alertar sobre amenazas al C^4 y asesorar con recomendaciones de contra-contramedidas.
   (2) Ataque de C2 que incluye:
      (a) Preparación de planes y ordenes deliberados y contingentes.
      (b) Preparación de listas de objetivos, apreciaciones y evaluaciones.
      (c) Analizar la amenaza e interpretar la situación, los nodos críticos, la vulnerabilidad ena, para derrotarlo y evaluación de daños de batalla.
   (3) Proporcionar apoyo de planeamiento de engaño de campo de batalla.

ANEXO 03 : CONSIDERACIONES DE PLANEAMIENTO DE SINFOR Y DE G-C^2

O1. PRINCIPIOS DE APOYO AL PLANEAMIENTO DE SINFOR

a. Los principios que guían al planeamiento de los SINFOR enfocan la atención de los planificadores sobre lo que es importante al cmdte. estos principios son:

(1) Modularidad
(2) Interoperatividad
(3) Oficiales de enlace
(4) Flexibilidad
(5) Economía
(6) Supervivencia
(7) Redundancia
(8) Estandarización
(9) Posibilidades comerciales
(10)Seguridad

b. Modularidad

(1) Los paquetes modulares de SINFOR consisten de un conjunto de equipo, de gente y software estructurado para un rango amplio de misiones. Los planificadores deben entender la misión, la intención del cmdte y el plan operacional, la disponibilidad de recursos y la estructura de información; que se requiere para enfrentar las necesidades de cada misión.

(2) Estos paquetes deben satisfacer las necesidades informacionales del cmdte durante la ejecución de fases de la misión. Los paquetes modulares de SINFOR deben ser flexibles, fácilmente extendible o escalable y estructurado de acuerdo a su capacidad y funcionalidad.

c. Interoperatividad

(1) La interoperatividad es la capacidad de los SINFOR para trabajar como un sistema. Implica compatibilidad de info común de fuerzas terrestres, conjuntas y hasta multinacionales, así como en sus procedimientos y elementos de datos.

(2) La interoperatividad es el fundamento sobre los cuales dependen las posibilidades de los SINFOR. Un SINFOR interoperable debe ser visible en todos los niveles funcionales como una infraestructura segura, casi perfecta y cohesiva; que satisfaga el C^2 y las necesidades de info de todos los escalones.

(3) Un SINFOR debería cumplir o estar acorde con la arquitectura técnica que se diseñe para todo el ejercito; es decir, que deben estar adheridos aquellos estándares y protocolares que ayuden a asegurar la interoperatividad y un intercambio de info, casi perfecto, entre las áreas funcionales del campo de batalla y fuerzas conjuntas.

d. Oficiales de enlace (OOEE)

(1) Los OOEE proporcionan un medio para que el cmdte y los planificadores incrementen la interoperatividad durante las diferentes fases de una opn y entre cmdtes y EEMM que previamente no han trabajado juntos.

(2) Los OOEE son especialmente importantes para interpretar la intención y lo relevante para los grupos a los que sirven, así como para superar la fricción natural que se desarrolla entre organizaciones dispares. Los OOEE facilitan la coordinación técnica y posibilitan a los planificadores administrar la info más eficiente y efectivamente.

e. Flexibilidad

Los planificadores deben ser flexibles cuando apoyan a las necesidades de info en situaciones cambiantes. Ellos deben anticipar la posibilidad de cambios en la misión o situación táctica y diseñar un plan para acomodarse a estos cambios.

f. Economía

Los sistemas empaquetados escalables facilitan la aplicación económica. Las restricciones en espacio, peso o tiempo limitan la cantidad o capacidad de los sistemas que pueden desplegarse. Las necesidades de info deben satisfacerse mediante la consolidación de facilidades funcionales similares integradas a sistemas comerciales.

g. Supervivencia

Los SINFOR deben ser confiables, robustos, elásticos y al menos tan perdurable como la fuerza que apoyan. Los sistemas distribuidos y los medios de comunicaciones alternos proporcionan una medida de elasticidad y flexibilidad. Los SINFOR deben estar organizados y desplegados para asegurar que funcionen gradualmente (y no catastróficamente) bajo grados de tensión. Los procedimientos de comando deben ser capaces de adaptarse para sobrellevar la tensión a pesar de la degradación o falla en los SINFOR.

h. Redundancia

Desde la perspectiva de una red de SINFOR, los planificadores proporcionan diversos enlaces sobre múltiple medios para asegurar el flujo de info oportuno. Desde la perspectiva del equipamiento, los planificadores aseguran que existan suficientes sistemas de respaldo y repuestos o partes, para mantener las capacidades de la red o sistema.

i. Estandarización

Las necesidades de info del cmdte no deben comprometerse por el uso de equipamiento no-estándard. Los planificadores deben asegurar que el equipo, su configuración y los sistemas operativos instalados incluyan un paquete modular estandarizado en el ejercito y de ser posible en la fuerza armada. La estandarización también incluye entrenamiento de SINFOR, simbología, diagramas de conmutación de red, diagramas de paquetes de red y terminología.

j. Posibilidades comerciales

(1) La disponibilidad de SINFOR comercial ofrece a menudo al cmdte una guía así como medios alternos, para satisfacer sus necesidades de C^2 informacional; pudiendo reducir la cantidad y tamaño de los paquetes modulares desplegados, sin embargo deberán considerarse aspectos de seguridad.

(2) El uso operacional de un sistema comercial permitirán a los planificadores compensar la falta de suficientes sistemas militares y enfrentar el surgimiento de necesidades de info en los primeras etapas de despliegue.

(3) El G-6 tendrá la responsabilidad de EM para la estandarización del equipamiento comercial y del software empleado sobre la Z/O. Sin embargo , los planificadores tendrán que asegurar el despliegue modular de los paquetes de SINFOR con arquitectura abierta, no propietaria, y con estándares y protocolos comúnmente aceptados para interfacear con sistemas comerciales.

k. Seguridad

El nivel de seguridad dependerá de la naturaleza de la información para su protección contra la amenaza de interceptación o explotación. Los aparatos de encriptado en línea o con seguridad de voz, usualmente proporcionarán seguridad de las comunicaciones. Por otro lado, el control del acceso físico a los terminales, software y CD's ayudarán a la seguridad de los SINFOR. La seguridad deberá ser balanceada con las necesidades de difundir información crítica rápidamente.

02. NECESIDAD DEL APOYO DE TELEMÁTICA PARA LOS SINFOR

a. Aspectos introductorios

(1) El apoyo de Telemática debe proporcionar los medios para transportar información desde la zona del interior, a través de salidas estratégicas hacia las unidades o elementos más adelantados que estén desplegados, para todas las etapas de la proyección de la fuerza.

(2) La necesidad del apoyo de Telemática para completar su misión será crítico para la ejecución exitosa de las OI y será dependiente de los factores METT-T. Las tareas/misión esencial del apoyo de Telemática a los SINFOR, están descritos en el Cap. 5 (párrafo 60); sin embargo el proceso de planeamiento de estos sistemas constará de cinco (05) fases que serán descritos en este anexo.

b. Fases del proceso de planeamiento de los SINFOR

(1) Las fases del proceso de planeamiento de los SINFOR consisten de los siguientes:

(a) Construir y proyectar los SINFOR.
(b) Extender los SINFOR.
(c) Dar forma a los SINFOR.
(d) Maniobrar los SINFOR.
(e) Reconstituir los SINFOR.

(2) Construir y proyectar los SINFOR (1ra fase)

(a) Los aspectos de seguridad que se derivan de ocupar un área dispersa son bastante estándares. Lo que será nuevo es la noción de establecer un centro de operaciones "santuario", es decir, un lugar desde el cual asegurar los SINFO de la unidad, que pudiera ser desde la zona del interior en instalaciones fijas o desde zonas un poco más adelantadas en cabinas sobre vehículos debidamente acondicionados con los medios de comunicaciones adecuados y seguros.

(b) Desde este "santuario", el apoyo de bases de datos y de EEMM proveen apoyo adicional para actividades tales como logística,

personal, telemedicina, juego de guerra, inteligencia básica, etc; “atrincherando” y protegiendo físicamente sus componentes y estableciendo un estricto control de emisión. El apoyo debería ser incluso desde el proceso de construcción del SINFOR, para las fuerzas de una GU que se está movimiento.

(3) Extender los SINFOR (2da fase)

(a) Las fuerzas de una GU se desplazan por múltiples rutas durante este período de extrema vulnerabilidad. Los cuarteles generales redundantes de C^2 deberían ser adelantados, donde los puestos de comando principal y alterno, tengan capacidades idénticas para comunicaciones, guerra electrónica e inteligencia; los cuales también deberán adelantarse, tanto para dar seguridad y para proporcionar apoyo a un reconocimiento de ruta.

(b) Los nodos de Telemática claves deberían posicionarse de manera adelantada para apoyar decididamente cuando la unidad empiece a maniobrar. Deberá observarse un control estricto sobre las misiones.

(c) Los sistemas de radares de redes de alerta temprana, de vigilancia, de reconocimiento y de ataque a objetivos aéreos o terrestres, pueden proporcionar conciencia situacional y seguimiento. Las plataformas aéreas con equipos retrasmisores de comunicaciones y los satélites pueden extender el alcance de las comunicaciones y redes, así como permitir que las unidades reciban actualización de info sobre el movimiento por medio radiodifusoras, que les facilitarán el inicio de la formación del espacio de batalla.

(4) Dar forma a los SINFOR

Cuando se piensa acerca de formar el espacio de batalla, uno debe entender la organización enemiga en su conjunto. Los objetivos, el ritmo, el escalón, las redes y las agrupaciones no son cosas físicas sobre el terreno; ellos son enteramente conceptos de C^2. Por ejemplo, si nuestra intención es hablar sobre "golpear" a la artillería enemiga, entonces es su capacidad de agrupar (para generar sus fuerzas planeadas y maniobrar con fuegos) que deseamos atacar.

(5). Maniobrar los SINFOR

(a) Sin una pausa en el ritmo del ataque, las unidades se moverán a un combate estrecho con fuerzas de maniobra. Las actividades de formación del espacio de batalla y SINFOR deberían de hecho ir aislando la actual zona de combate (o batalla) estrechando la capacidad de reconocimiento enemiga. El combate decisivo será posible sin enfrentar a una fuerza enemiga en detalle. Esto será alcanzado mediante la concentración del poder de combate en ubicaciones precisas que destruyan la integridad organizacional de la fuerza. La capacidad de seguimiento de una fuerza y las herramientas predictivas permitirán maniobrar "donde no está el enemigo y orquestar los efectos no donde él está, sino donde él estará. El proceso de inteligencia buscará el punto de intersección y los colectores u órganos de búsqueda orgánicos contribuirán a ello.

(b) El cmdte estará atento a como reaccionará el eno a su plan. La conciencia situacional completa será crítica. Las redes de

comunicaciones y/o Internet táctica deben ser maniobrables para mantener las capacidades del flujo de info y comunicaciones necesarias a un ancho de banda adecuado que necesita el esfuerzo principal. Durante las opns decisivas, el flujo de info llegará a crecer, consecuentemente habrá una sobre-carga de info, por lo que las NICC llegarán a jugar un rol muy importante en la frecuencia y características de ciertos informes; enfocándose en la visualización de la secuencia de eventos que conduzcan al cmdte desde su situación actual al estado final.

(6) Reconstituir los SINFOR

Los SINFOR son consolidados y reconstituidos para limpiar los dígitos indeseados en el campo de batalla, mediante la reparaciones en la Internet, limpieza y "purgado " de base de datos. Las direcciones y protocolos deberán ajustarse a la reorganización actual, reflejando las perdidas que hubiera. Las fuerzas se comunicarán a través de los SINFOR por telemantenimiento y tele-medicina, así como llamadas radiales/telefónicas normales. En esta fase se da inicio al reposicionamiento de los SINFOR para las ramificaciones y secuelas (contingencias).

03. PROCESO DE PLANEAMIENTO DE G-C^2

a. En casi cada caso, los cmdtes del ejército emplearán la G-C^2 dentro de un contexto conjunto; sin embargo sea que una opns sea conjunta o puramente del ejército, el cmdte conducirá la G-C^2 en su organización. El oficial de EM de operaciones (C-3/G-3) planeará y ejecutará las opns de G-C^2.

b. El proceso de cmdo y EM para las opn de G-C^2 no serán diferentes de cualquier otro, excepto en los parámetros en que se enfoca. De igual manera el planeamiento conjunto de la G-C^2 y los procesos que siguen se aplicarán a todos los niveles de la guerra y escalones.

c. Planeamiento conjunto de G-C^2

(1) Siendo la G-C^2 inherentemente conjunta; el desarrollo de capacidades, planes, programas, tácticas, conceptos de empleos, inteligencia y apoyo de comunicaciones en opns de G-C^2; como parte de la estrategia militar, requerirá coordinación con las diferentes componentes que intervienen. Un intercambio de oficiales de enlace puede ser lo más efectivo para asegurar estas coordinaciones.

(2) La fuerza conjunta y/o la fuerza terrestre conducirán las esfuerzos de G-C^2 alrededor de la organización de G-C^2 que apoya a esa fuerza, que puede ser una celda o negociado especial (en opns conjuntas) o un EM de batalla (para el ejercito). Para un empleo conjunto de la G-C ^{2} la clave será el balanceo de las posibilidades de los institutos o componentes de la fuerza y de los elementos de la G-C^2. Sólo conforme exista una sinergía en el empleo de elementos de una manera organizada, habrá una sinergía en la organización de las posibilidades de los componentes para enfocarse en el cumplimiento de la misión.

d. Planeamiento del EM de batalla

(1) Pasos del planeamiento de atq´-C^2 .- Son siete:

(a) Identificar como el ataq'-C^2 podría apoyar la misión total y al concepto de opns. El producto será "la misión de G-.C^2"
(b) Identificar los sistemas de C^2 enemigos cuya degradación tendrá un efecto significativo sobre el C^2 eno. Su producto será "una lista de objetivos potenciales de C^2 enemigos".
(c) Analizar los sistemas de C^2 enemigos para nodos vulnerables y críticos. Su producto será "Una lista de objetivos de alto valor (OAV)".
(d) Priorizar los nodos para su degradación. Su producto será "una lista de objetivos de alto costo (OAC)".
(e) Determinar el efecto deseado y como los elementos de G-C^2 contribuirán al objetivo en su conjunto. Su producto será "el concepto de opn de G-C^2".
(f) Asignar recursos a cada nodo de C^2 eno que se ha designado como objetivo. Su producto será "la asignación de objetivo a unidades subordinadas".
(g) Determinar la efectividad de la opn. Su producto será "la evaluación de daños de batalla".

(2) Pasos del planeamiento de prot-C^2.- Son siete:
(a) Identificar como la prot-C^2 podría apoyar a la misión en su conjunto y al concepto de opns. Producto: "misión de G-C^2".
(b) Por fases, identificar los sistemas críticos de C^2 amigo que apoyan a la misión y concepto de opns. Producto: "lista de C^2 amigo".
(c) Determinar las posibilidades enas para conducir atq'-C^2 y los efectos del atq'-C^2 amigo sobre nuestros sistemas de C^2 (interferencia mutua). Producto: "evaluación de la amenaza".
(d) Analizar los sistemas de C^2 amigo para nodos críticos y vulnerables. Producto: "Identificación de nodos amigos críticos y vulnerables".
(e) Priorizar los nodos amigos que serán protegidos. Producto: "Concepto de opn de prot-C^2".
(f) Recomendar medidas de protección para los nodos. Producto: "Tareas a las unidades subordinadas".
(g) Monitorear la efectividad del plan de prot-C^2. Producto: "evaluación de daños de batalla".

ANEXO 04: PROPUESTA DE ORGANIZACIÓN DE CELDA O NEGOCIADO DE OPERACIONES DE INFORMACION

01. INTRODUCCION

Basado en las consideraciones de los factores METT-T, el Cmdte puede designar una celda o negociado dentro de su EM. La estructura de la celda será prerrogativa del cmdte, pudiendo ser algo tan simple como una función a tarea adicional a una de los miembros de su EM (Normalmente al G-3 o al G-6 o una conjunción de elementos de ambos) o una aproximación más formal estableciendo una celda permanente con miembros designados específicamente. Esta celda de OI normalmente estará basada en el nivel o escalón de la fuerza.

02. ORGANIZACIÓN

a. La celda de OI debería contar con representantes de todos sus elementos que integran y sincronizan sus recursos, particularmente los de G-C^2. Estos representantes de elementos podrían ser: asuntos civiles (G-5), relaciones públicas, opns/sicolog, Guerra Electrónica, comunicaciones, inteligencia, apoyo de fgos y de operaciones.

b. Las funciones de la celda de OI incluirían:

(1) Planear el esfuerzo total de OI para el Cmdte.

(2) Desarrollar conceptos de OI para apoyar al esquema de maniobra.

(3) Establecer prioridades de OI para cumplir los objetivos planeadas.

(4) Determinar la disponibilidad de recursos de OI para llevar a cabo los planes.

c. La consolidación de tareas ayudarán en la integración y sincronización que se requiere para las OI efectivas, incluyendo la coordinación con la comunidad de G-I conjunta

d. Conforme el espectro de encuentros o combates se mueve desde época de paz hacia la guerra, podría ser más apropiado establecer un EM de batalla para OI (EMBOI) para niveles de GU y superiores; aunque sus funciones relativamente podrían ser las mismas que la celda de OI, este EM tendría un propósito más amplio dentro del contexto de una campaña como se explicó en el anexo 01 y como se muestra en la figura siguiente:

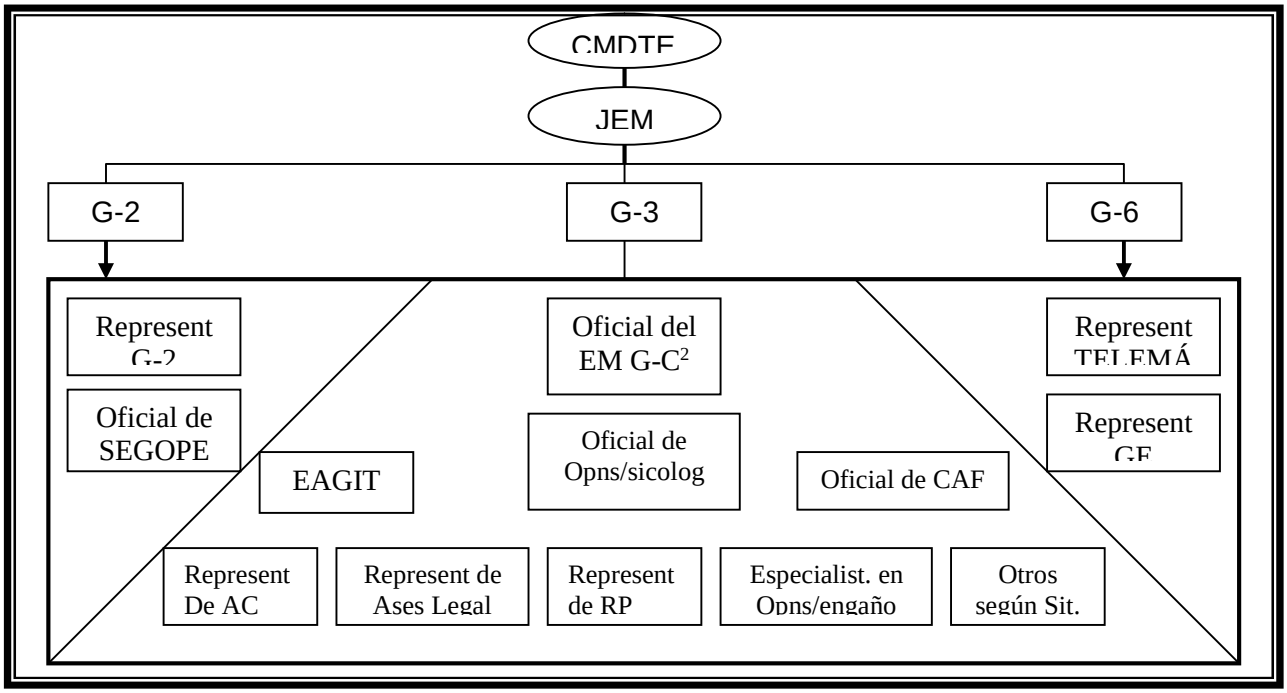

Figura: NOCION DE UN EM DE BATALLA PARA OI (EMBOI)

03. ENTRENAMIENTO

a. Cuando se empleen OI en ejercicios tácticos o de campaña, será importante tener en consideración lo siguiente:
   (1) Desarrollar objetivos de OI concretos y alcanzables.
   (2) Proporcionar suficientes elementos de OI para apoyar los objetivos del ejercicio.
   (3) Crear un ambiente tan realístico como sea posible para el ejercicio de OI.
   (4) Evaluar el empleo de actividades de OI.
   (5) Ejercitar las seis actividades de OI (obtención, empleo, protección, manejo, explotación y negación) en el contexto del ejercicio.
   (6) Usar apropiadas medidas de seguridad para proteger a los elementos de OI.
   (7) Evaluar el uso de productos con apoyo de computador para ejecutar OI (herramientas de sincronización)
   (8) Ejercitar los cinco elementos de la G-C^2 (GE, SEGOPE, ENGAÑO, Opns/Sicolog y destrucción) en el contexto del ejercicio.

b. Inicialmente, las OI efectivas requerirán de productos de info específica sobre aspectos y antecedentes militares (C^2, inteligencia, GE y capacidades), sociales, religiosos y económicos del adversario; que pueden ser proporcionados por los planificadores del ejercicio. En segunda instancia, la fzas opuestas deberían tener una capacidad de OI consistente con el P/O o escenario del plan de contingencia que será la base para el ejercicio. Finalmente, consistente con los fines del ejercicio, debería permitirse un juego libre de OI para ambos lados; inclusive promover caos de C^2 para evaluar el grado de habilidad de los participantes que permitan ganar experiencias valiosas que demanden creatividad y agilidad mental.

c. Una lista de tareas esenciales o misiones de OI deberían incluirse considerando a cada componente (opns propiamente dichas, IRI y SINFOR). Esta lista mejorará el objetivo de alcanzar el dominio de la información en lugares y tiempos seleccionados durante una opn. Estas tareas incluyen:
   (1) Determinar la info que se requiere para las OI y como obtener rptas:
      (a) Identificar los NICC para OI , los NPI, los objetivos de alta prioridad y la sincronización de los planes de inteligencia e info sobre una base de tiempo casi real.
      (b) Establecer enlaces de info estratégicos, operacionales y tácticos para los órganos de búsqueda, reunión y para los procesos de tramitación de informes, para desarrollar una PIC de OI continua y oportuna.
   (2) Conocer sus capacidades de OI y vulnerabilidades al eno, el ambiente natural, la política establecida, la ley internacional, etc.
      (a) Proveer un modelo y simulación para el entrenamiento y evaluación del rendimiento, ensayo de la misión y toma de decisiones.
      (b) Identificar y priorizar los EEIA para OI.
   (3) Conocer las capacidades de OI enemigas y sus vulnerabilidades :
      (a) Mantener una apreciación continúa de OI de los adversarios potenciales y/o otras situaciones operacionales en apoyo de la conciencia situacional de OI y visualización del campo de batalla.
      (b) Evaluar continuamente las opns de $C^4I/G\text{-}C^2$ adversaria, sus fortalezas y vulnerabilidades.
   (4) Conocer como ve el eno sus capacidades y vulnerabilidades en términos de OI, el campo de batalla y NPI:
      (a) Entender el proceso de toma de decisiones eno.
      (b) Identificar los nodos de OI críticos del eno.
      (c) Desarrollar los perfiles de personalidad de los líderes enos.
      (d) Entender la doctrina de toma de decisiones ena, sus tácticas y sus procedimientos operativos vigentes.
   (5) Proteger las OI críticas y vulnerabilidades amigas:
      (a) Establecer procesos de fuente abierta para obtener, procesar, proveer, dar seguridad y eliminar info crítica de OI, incluyendo AC, RP, info gubernamental y no-gubernamental dentro de las limitaciones legales y políticas.
      (b) Establecer y mantener redes críticas, seguras, inter e intra TO y de comunicaciones y computadoras militares que apoyen a las OI; por ejemplo, digitación, conciencia situacional, visualización del campo de batalla, CCR, distribución y C^2 a través del espacio de batalla.
      (c) Evaluar continuamente las vulnerabilidades de C^2 amiga y opns de prot-C^2; ajustándolas para mantener la efectividad de C^2.
      (d) Alcanzar la prot-C^2 en apoyo de la protección de la integridad e infraestructura de datos, nodos de OI/C^2, control y superioridad del espectro electromagnético y degradación armónica.
      (e) Establecer procedimientos para recuperar el dominio de la info, sí es que se hubiese perdido.
   (6) Atacar las vulnerabilidades críticas de OI enas:

(a) Establecer los objetivos para el ataq'-C^2 y de evaluación de daños de batalla, implementando enlaces para difundir expeditivamente info del adversario.
(b) Atacar, negar, degradar, explotar y/o influir las posibilidades u otras opns de $C^4I/G\text{-}C^2$ adversario empleando medios letales y no-letales.

ANEXO: 05 GLOSARIO DE TERMINOS RELACIONADOS A LAS OPERACIONES DE INFORMACION

- A -

ACUERDO DE ESTATUS DE LA FUERZA .- Un acuerdo que define la posición legal de una fuerza militar visitante desplegada en el territorio de un país amigo, aunque este acuerdo sea bilateral o multilateral. Las provisiones pertenecientes al estatus de una fza visitante pueden estas sentadas ya sea en un acuerdo separado o pueden formar parte de un acuerdo más comprensivo. Estas provisiones describen como las autoridades de una fza visitante pueden controlar a los miembros de esa fuerza y la responsabilidad o sometimiento de la misma o sus miembros a las leyes locales o a las autoridades locales oficiales. Por extensión, aquel acuerdo que delinea asuntos que afectan las relaciones entre una fuerza militar y las autoridades civiles y población, considerándose como acuerdos de asuntos civiles.

ADMINISTRACION DEL RIESGO .- Es el proceso de detectar, evaluar y controlar el riesgo que surja de los factores operacionales y toma de decisiones; que balancee el costo del riesgo con los beneficios de la misión. Los cinco pasos de la administración del riesgo son: identificar los peligros, evaluar los peligros, desarrollar controles y tomar decisión del riesgo, implementar controles, y supervisar y evaluar (Ver ME 11-30, Organización y Opns de EM de Com Ed. 1999).

ADVERSARIO .- Es un término empleado a menudo en este y otros manuales en lugar de enemigo, para diferenciar este último que indica a aquel adversario enganchado en operaciones letales contra las fuerzas nacionales.

AMBIENTE DE INFORMACION GLOBAL (AIG).- Todos los individuos, organizaciones y sistemas de información; muchos de los cuales están fuera de la esfera y control de las autoridades de comando nacional y militar, que obtienen, procesan y/o difunden información a las audiencias nacionales e internacionales.

AMBIENTE DE INFORMACIÓN MILITAR (AIM).- Es aquel ambiente contenido dentro del ambiente de información global; consistente de individuos, organizaciones y sistemas de información; tanto amigos como del adversario, militares y no-militares; que soportan, posibilitan o influencian significativamente; una operación militar específica.

AMBIENTE OPERATIVO COMUN.- Aquel que le proporciona al cmdte una mirada, toque, sonido o sentido familiar, sin importar donde este desplegado. El interface entre el sistema de C^4I y la presentación de la info serán consistentemente mantenidos de plataforma a plataforma, posibilitando al cmdte centrar su atención sobre la crisis que estuviera manejando.

APLIQUES.- Una familia de computadoras de tamaño laptop conectadas a aparatos de navegación (GPS) y radios, para proporcionar capacidades de procesamiento y proyección hacia plataformas, sin un procesador insertado.

APOYO DE GUERRA ELECTRONICA (AGE) .- Una división de la GE que envuelve acciones misionadas por o bajo el control directo de un cmdte operacional para buscar, interceptar, identificar y localizar fuentes de radiación de energía electromagnética intencional y no intencional; con el propósito de reconocer una amenaza inmediata. El AGE proporciona información que se requiere para decisiones inmediatas que envuelvan opns de GE y otras acciones tácticas tales como eludir una amenaza, considerarla como objetivo y buscarla.

APRECIACION.- Son conclusiones personales, estimaciones oficiales y suposiciones sobre otro grupo de intenciones, posibilidades y actividades; empleadas en un proceso de planeamiento y/o de toma de decisiones.

ATAQUE DE COMANDO Y CONTROL (Atq´- C^2).- Es la ejecución sincronizada de acciones tomadas para alcanzar objetivos establecidos que impidan el C^2 efectivo del adversario mediante la negación de info, la influencia, la degradación o la destrucción del sistema de C^2 adversario.

- B -

BASE DE DATOS DE INFORMACION.- Es la visualización de un sistema futuro donde los cmdtes y sus unidades podrán accesar y actualizar continuamente una base de datos común de información relevante (por ejemplo de logística, inteligencia, movimientos, personal, etc).

BATALLAS .- Consiste de una serie de encuentros o combates relacionados, que duran mucho más que un combate, envuelve fuerzas de gran magnitud y que podrían afectar el curso de la campaña. Ellas ocurren cuando la división, el Ejército de Operaciones o el cmdte del componente terrestre del Teatro de Operaciones pelea o lucha por objetivos significativos. Las batallas pueden ser cortas en duración y llevadas a cabo en áreas relativamente pequeñas, o pueden durar semanas y cubrir grandes áreas. (Ver campañas, combates y operaciones mayores).

- C -

COMANDO DE BATALLA.- El arte de tomar decisiones y liderar en la batalla (cbte). Ello incluye controlar las opns y motivar a las tropas y sus organizaciones en una acción coordinada para cumplir misiones. Incluye también la visualización del estado actual y un estado futuro, para que mediante la formulación de conceptos de opns se consiga llegar desde el uno al otro lado al menor costo posible. Se considera como sistema operacional del campo de batalla que incluye la asignación de misiones, la priorización y la distribución de recursos, la selección de tiempos y lugares críticos para actuar y el conocimiento de cómo y cuando realizar ajustes durante la batalla (cbte).

COMANDO, CONTROL, COMUNICACIONES, COMPUTACION E INTELIGENCIA (C^4 I).- Es un sistema que integra la doctrina, procedimientos, estructuras organizacionales, facilidades e instalaciones, comunicaciones y computadoras y

apoyados por los recursos de inteligencia. Incluye sistemas de alerta temprana, sensores remotos, estaciones terrenas satelitales para fines diversos, radares de diferentes usos y otros equipos electrónicos, integrados en redes de telecomunicaciones enlazando nodos que sirvan a puestos de comando o cuarteles generales autorizados. El C^4 I proporciona a las autoridades de comando en todos los niveles o escalones con sistemas de datos precisos y oportunos, para planear, monitorear, dirigir, controlar e informar operaciones. Son los medios que emplea el cmdte para comunicar su intención, comandar y controlar sus fzas y difundir info pertinente a toda su zona de opns.

COMANDO DE COMPONENTE FUNCIONAL.- Un comando, normalmente compuesto de dos o más elementos de diferentes institutos (pero no necesariamente), que puede establecerse a través de todo el rango de operaciones militares para realizar misiones operacionales particulares, que pueden ser de corta duración o pueden extenderse un período de tiempo.

COMANDO DE COMPONENTE DE INSTITUTO.- Un comando consistente de un Cmdte de un componente en un TO y todas aquellas fuerzas de su instituto bajo su comando, incluyendo las de apoyo que han sido asignadas a un Comando combatiente o que serán asignadas más adelante a subordinados comandos unificados o fuerzas de tarea conjunta.

COMANDO Y CONTROL (C^2) .- El ejercicio de la autoridad y dirección por un Comandante apropiadamente designado, sobre fuerzas asignadas y agregadas en el cumplimiento de la misión. Las funciones del C^2 son realizadas mediante un arreglo de personal, equipo, comunicaciones, instalaciones y procedimientos empleados por un comandante durante el planeamiento, dirección, coordinación y control de las fuerzas y las operaciones en el cumplimiento de la misión.

COMANDANTE COMBATIENTE.- Un Cmdte de un comando unificado o específico establecido por resolución suprema.

COMANDO UNIFICADO.- Un comando con una amplia y continua misión bajo un único Comandante y compuesto de componentes asignados significativos de dos o más institutos armados y que está establecido o designado por Resolución Suprema. Es también llamado comando combatiente unificado.

COMUNICACIONES.- Como se emplea en este manual, es un método o medios de trasladar info de cualquier clase de una persona o lugar a otra.

CONCIENCIA SITUACIONAL.- Es una condición que se alcanza respecto a: un entendimiento común de la evaluación de la situación, la intención y el concepto de operaciones del Cmdte; combinado con un cuadro claro de los dispositivos y capacidades de las fuerzas amigas y enemigas.

CUADRO COMUN RELEVANTE (CCR).- Cuando es referido a un campo de batalla, es la agrupación de datos que son compartidos entre todas las fuerzas amigas, sobre el dispositivo de las fuerzas amigas y enas. Estos datos son empleados para construir una estructura gráfica relevante proyectada al combatiente, que mejorará

en detalle lo mostrado conforme el elón apoyado es más cercano al soldado; comúnmente es llamado conciencia situacional.

- D -

DECISION DEL RIESGO.- La decisión de aceptar o no el riesgo (s) asociados con una acción; que es realizada o tomada por un cmdte, líder o individuo responsable por la ejecución de esa acción.

DESARTICULAR.- Una tarea táctica u efecto del obstáculo que integra el planeamiento de los fuegos y los esfuerzos de los obstáculos para dislocar o quebrar una formación enemiga; retardar su ritmo; interrumpir la programación enemiga; causar un prematuro compromiso de fzas enas; o el desarrollo irregular o poco sistemático de su ataque.

DESTRUCCION .- (1) Cuando se refiere a los efectos de los fgos de artillería de campaña, será un objetivo puesto fuera de acción permanentemente o con por lo menos 50% de bajas o daño sobre su material. La destrucción requiere de grandes consumos de munición y según convención y tratados internacionales solo es permitido si se emplean municiones y armas convencionales. (2) Cuando se refiere a la misión de helicópteros de ataque, será el porcentaje de vehículos destruidos o inutilizados que debe ser especificado por el escalón superior.

DESTRUCCION FISICA.- Es la aplicación de la potencia combativa para destruir o neutralizar instalaciones y fuerzas enemigas. Incluye fuegos directos o indirectos desde fuerzas terrestres, navales o aéreas, así como las acciones directas ejecutadas por fuerzas de operaciones especiales.

DESTRUIR.- (1) Una tarea táctica para rendir físicamente una fza de cbte ena a nivel de ineficiencia al menos que sea reconstituida. (2) Someter un objetivo a tal daño que no pueda funcionar ni restablecerse a su condición utilizable o empleable sin antes ser totalmente reparado o reconstituido.

DINAMICAS DE BATALLA.- Son áreas significativas que definen los cambios que pueden producirse en las operaciones de una fuerza moderna desde sus operaciones actuales. Estas dinámicas son: comando de batalla, espacio de batalla, profundidad y ataque simultaneo, entrada inicial y apoyo logístico.

DOMINIO DE LA INFORMACION .- Es el grado de superioridad de la información que permite al poseedor el empleo de los sistemas de información y sus posibilidades para lograr una ventaja operacional en un conflicto o para controlar la situación en la estabilidad y soporte de las operaciones, al mismo tiempo que niega estas posibilidades al adversario.

- E -

ELEMENTOS ESENCIALES DE INFORMACION AMIGA (EEIA) .- Preguntas claves probablemente para ser respondidas por los sistemas de inteligencia y oficiales adversarios, sobre intenciones específicas, posibilidades y actividades amigas; de tal manera que ellas puedan obtener respuestas críticas a su efectividad operacional. Son aspectos críticos de una operación amiga que de ser conocidos por el enemigo, podrían subsecuentemente comprometer, llevar al fracaso o limitar el éxito de la operación; y, por lo tanto deben ser protegidos de la detección enemiga.

ENGAÑO.- Son aquellas medidas diseñadas para inducir a error al oponente mediante la manipulación, distorsión o falsificación de evidencia; para llevarlo a reaccionar de una manera perjudicial a sus intereses. El objetivo del engaño es hacer que un oponente sea más vulnerable a los efectos de las armas, la maniobra y opns de las fzas.

ENGAÑO MILITAR.- Son acciones ejecutadas para desorientar deliberadamente a los que toman decisiones militares en el adversario; sobre las capacidades, intenciones y opns militares amigas; causando de ese modo que el adversario tome acciones específicas (o inacciones) que contribuirán al cumplimiento de la misión amiga.

ESPACIO DE BATALLA .- Es conceptualmente un volumen físico dentro del cual un cmdte busca dominar al eno. Este espacio se expande o contrae en relación a la habilidad del cmdte para encontrar y enfrentar al eno, o puede cambiar conforme la visión del campo de batalla del cmdte cambia. Incluye o contiene la visión tridimensional del campo de batalla (frente, profundidad y altura) y el espectro electromagnético, sobre el cual el cmdte posiciona y mueve sus recursos; y está influenciado por las dimensiones operacionales de cbte (tiempo, ritmo, profundidad y sincronización). No está asignado por el elón sup ni está restringido por límites asignados. Sin embargo a nivel táctico está determinado por el alcance de los sistemas de fuego directo y el terreno en el cual ellos son aplicados.

EVALUACION DEL RIESGO.- Es la identificación y evaluación de peligros. Son los dos primeros pasos del proceso de administración del riesgo (Ver administración del riesgo).

EXPLOTACIÓN.- (1) Tomar ventaja total de cualquier información obtenida para propósitos tácticos, operacionales o estratégicos. (2) Tomar ventaja total de los éxitos en batalla y continuar los beneficios iniciales. (3) Una opn ofensiva que usualmente sigue a un atq´ exitoso y que está diseñada para desorganizar al eno en profundidad.

- F -

FUNCIONES DE COMBATE.- Aquellas que los cmdtes integran y coordinan para sincronizar los efectos de batalla en tiempo, espacio y propósitos. Estas son: inteligencia, maniobra, apoyo de fuego, defensa aérea, movilidad y supervivencia, logística y comando de batalla. (Ver ME 11-30, glosario de términos y sistemas operacionales del campo de batalla).

- G -

GUERRA DE COMANDO Y CONTROL (G-C²) .- El empleo integrado de seguridad de las operaciones (SEGOPE), engaño militar, operaciones psicológicas, guerra electrónica y destrucción física; apoyados mutuamente por la inteligencia; para negar información, influir, degradar o destruir las posibilidades de comando y control (C^2) adversario; mientras protegemos las posibilidades del C^2 amigo contra sus acciones. La G-C^2 es una aplicación de la guerra de información en operaciones militares y a la vez es un componente de la misma. La G-C^2 se aplica a través de todo el rango de operaciones .militares y en todos los niveles de un conflicto. La G-C^2 es tanto ofensiva como defensiva : a) **Ataque de C²** .- Es el efectivo impedimento del comando, control y comunicaciones (C^3) de las fuerzas adversarias, mediante la negación de información, la influencia, la degradación o la destrucción del sistema C^3 adversario. b) **Protección de C²** .- Es el mantenimiento efectivo del C^2 de nuestras propias fuerzas transformándolas en ventajas amigas o impidiendo que los esfuerzos enemigos intenten que obtengamos información, influir, degradar o destruir nuestro sistema de C^3.

GUERRA DE INFORMACION (G-I).- Son las acciones tomadas para alcanzar superioridad de información mediante la afectación de la información del adversario, de sus procesos basados en información y de las redes y/o sistemas basados en computadora; al mismo tiempo que defendemos nuestra propia información, nuestros procesos basados en información y sistemas de información.

GUERRA ELECTRONICA (GE).- Cualquier acción militar que envuelva el empleo de energía directa y electromagnética para controlar el espectro electromagnético (ESELECMAG) o para atacar al eno. Las tres mayores subdivisiones de la GE son: medidas de apoyo de guerra electrónica (MAGE); contramedidas electrónicas (COME) o ataque electrónico; y contra-contramedidas electrónicas (COCOME) o protección electrónica. También se le puede definir como el uso de energía electromagnética para determinar, explotar, reducir o prevenir el empleo hostil del espectro electromagnético y asegurar el empleo amigo del mismo.

- I -

INDICADOR AMIGO.- Es una actividad que puede contribuir a la determinación de una de nuestras formas de acción y que los analistas de SEGOPE deben buscarlo, analizarlo y hacer
apreciaciones de si dicho indicador puede revelar posibilidad, vulnerabilidad e intención.

INFOESFERA.- El rápido crecimiento de redes globales militares; y, de redes y sistemas de C^4 comerciales, enlazando bases de datos de info y centros de fusión que serán accesibles al combatiente en cualquier lugar y en cualquier momento, en la realización de cualquier misión; proporcionando apoyo a fuerzas conjuntas con un backbone de intercambio de info automatizado, global, seguro y transparente. Esta posibilidad emergente será altamente flexible para apoyar a las infraestructuras de C^2 adaptivas del siglo XXI.

INFORMACIÓN DE COMBATE.- Datos no evaluados, obtenidos o proveídos directamente a un cmdte táctico que, debido a su naturaleza altamente perecedera o a lo crítico de la situación; no puede ser procesada para inteligencia táctica del usuario.

INFORMACION RELEVANTE.- Información extraída del ambiente de información militar (AIM) que significativamente impacta, contribuye o está relacionada a la ejecución de la misión operacional en curso.

INFORMACION.- Datos, hechos o instrucciones reunidos desde un ambiente y procesados en cualquier medio o forma utilizable.

INFORMACION CRITICA.- Son hechos específicos sobre intenciones, capacidades y actividades amigas que necesita vitalmente un adversario para su planeamiento y acción efectiva, de tal forma de garantizarle el fracaso o consecuencias inaceptables para el cumplimiento de la misión amiga.

INFRAESTRUCTURA .- (1) Las facilidades básicas, equipamiento e instalaciones necesarias para el funcionamiento de un sistema, una red o una red integrada. (2) Un término generalmente aplicable a todas las instalaciones fijas y permanentes, fábricas o facilidades para el apoyo y control de fzas militares.

- J -

JUEGO DE GUERRA.- Una simulación, por cualquier medio, de una operación militar que envuelve 2 o más fuerzas opuestas, usando reglas, datos y procedimientos diseñados para describir una situación actual o asumida de la realidad. Un proceso paso a paso de acción, reacción y contracción para visualizar la ejecución de cada F/A amiga en relación a FF/A enas y reacciones. Explora las posibles ramificaciones o secuelas al plan principal resultante en un plan final y puntos de decisión para acciones críticas (Ver visualización del campo de batalla)

- M -

MEDIDAS DE APOYO DE GUERRA ELECTRONICA (MAGE).- Ver Apoyo de guerra electrónica.

MEDIOS ADMINISTRATIVOS DE ENGAÑO.- Son recursos, métodos y técnicas para convertir o negar evidencia verbal, pictográfica, documentaria u otra de similar naturaleza; a una potencia extranjera.

MEDIOS DE ENGAÑO.- Son los métodos, recursos y técnicas que pueden emplearse para convertir información a el objetivo de engaño. Hay tres categorías de medios de engaño:. Medios físicos, medios técnicos y medios administrativos.

MEDIOS FISICOS DE ENGAÑO.- Son actividades y recursos empleados para convertir o negar información seleccionada a una potencia foránea (Ejms: opns

militares, incluyendo ejercicios de campaña, reconocimientos, actividades de entrenamiento y movimiento de fzas; empleo de equipo y artificios falsos o fantasmas; tácticas; áreas o zonas de servicio; actividades logísticas, tales como acumulación de abastecimientos de algunas clases, reparaciones en campaña; y, pruebas y evaluación de actividades).

MEDIOS TECNICOS DE ENGAÑO.- Son recursos de materiales militares y sus técnicas de operación asociadas empleadas para convertir o negar info seleccionada a una potencia extranjera a través de la deliberada radiación, reradiación, alteración, absorción o reflexión de energía; la emisión o supresión de olores químicos o biológicos; y, la emisión o supresión de partículas radioactivas.

- N -

NECESIDADES DE INFORMACION CRITICA DEL COMANDANTE (NICC).- Aquella info requerida por el cmdte que afecta directamente sus decisiones y dicta la ejecución exitosa de opns tácticas u operacionales. Las NICC normalmente son el resultado de tres tipos de necesidades de info: necesidades prioritarias de inteligencia (NPI), elementos esenciales de info amiga (EEIA) y necesidades de info de las fzas amigas (NIFA).

NECESIDADES PRIORITARIAS DE INTELIGENCIA (NPI).- Aquellas necesidades de inteligencia por las cuales un Cmdte tiene una prioridad anticipada y establecida en su tarea de planeamiento y toma de decisiones. Las NPI son iguales a los elementos esenciales de información (EEI).

NIVEL OPERACIONAL.- Aquel nivel de la guerra en que fzas conjuntas y/o combinadas, dentro de un teatro de opns (TO) o zona de opns (Z/O); planean, conducen y sostienen las campañas y opns mayores para conquistar los objetivos estratégicos de un comando unificado o autoridad militar mayor. Las actividades en este nivel enlazan la táctica y estrategia mediante el establecimiento de: objetivos operacionales que se necesitan para cumplir los objetivos y/o propósitos nacionales y/o estratégicos, la secuencia de eventos para alcanzar los objetivos operacionales, las acciones iniciales, y la aplicación de los recursos para sostener estos eventos. Estas actividades implican una dimensión de tiempo y/o espacio más amplia que la requerida en la táctica; ya que deben asegurar el apoyo logístico con anticipación para las fzas tácticas y proporcionarle los medios por los cuales los éxitos tácticos serán explotados para lograr objetivos estratégicos.

- O -

OPERACIÓN DE ENGAÑO.- Una opn militar conducida para inducir a error al oponente.

OPERACIONES DE INFORMACION (OI).- Son operaciones militares continuas dentro del ambiente de información militar (AIM) que posibilita, mejora y protege la habilidad de las fuerzas amigas para reunir, procesar y actuar sobre la información para alcanzar una ventaja a través de todo el rango de las operaciones militares. Las

IO incluyen la interacción con el ambiente de información global (AIG) y la explotación o negación de información y posibilidades de decisión de un adversario.

OPERACIONES DE NO - GUERRA .- Son actividades militares realizadas durante época de paz y/o conflicto que no necesariamente involucra choques armados entre dos fzas organizadas.

OPERACIONES SICOLOGICAS.- Son aquellas que trasladan información seleccionada e indicadores hacia audiencias foráneas para influir sus emociones, motivaciones, razones objetivas y finalmente, la conducta de gobiernos extranjeros, organizaciones, grupos e individuos. Su propósito es inducir o reforzar actitudes y conductas foráneas favorables a los objetivos del promotor.

- P -

PERTURBACION.- La deliberada radiación, reradiación o reflexión de energía electromagnética para prevenir o degradar la recepción de información por un receptor. Incluye la perturbación de equipos de comunicaciones y no-comunicaciones.

PROPAGANDA.- Cualquier forma de comunicación en apoyo de objetivos nacionales diseñadas para influir opiniones, emociones, actitudes o conductas de cualquier grupo para beneficiar al promotor, directa o indirectamente.

PROTEGER.- (1) Una tarea táctica para prevenir la observación, el encuentro o la interferencia con una fza o lugar. (2) Todas las acciones tomadas para resguardase contra el espionaje o captura de información y equipo sensible.

PROTECCION DE COMANDO Y CONTROL (Prot-C^2).- Es el mantenimiento del C^2 efectivo de las propias fzas tornándola en ventaja amiga o negando a los esfuerzos del adversario su capacidad de negar, influir, o degradar la info o de destruir el sistema de C^2 amigo. La prot-C^2 puede ser de naturaleza ofensiva o defensiva; en el primer caso, emplea los cinco elementos de la G-C^2 (SEGOPE, engaño, GE, opns/sicolog y destrucción) para reducir la habilidad adversaria de conducir atq´-C^2; y en el segundo caso, reduce las vulnerabilidades del C^2 amigo al atq´-C^2 adversario mediante el empleo adecuado de la protección física, electrónica y de inteligencia.

PROTECCION DE LA FUERZA.- Cualquier reunión o combinación de medidas para prevenir o mitigar el daño, desbaratamiento o dislocación a una agrupación de personal militar, sistemas de armas, vehículos, instalaciones o apoyos.

PROTECCION ELECTRONICA.- También llamado contra-contramedidas electrónicas (COCOME) es una parte de la GE que envuelve acciones que se toman para proteger al personal, facilidades y equipo, de cualquier efecto del empleo de GE amiga o enemiga que degrade, neutralice o destruya las capacidades de combate amigo.

- R -

RANGO DE OPERACIONES MILITARES.- Dentro de un contexto estratégico, son un conjunto de actividades militares o no. que realiza el ejército en tres ambientes diversos (paz, conflicto y guerra) para alcanzar objetivos estratégicos nacionales en coordinación con otras fuerzas armadas y/o sincronizadamente con todos los elementos del poder nacional.

REGLAS DE ENCUENTROS .- Ver reglas de compromiso.

REGLAS DE COMPROMISO .- Son directivas emitidas por una autoridad militar competente que delinea las circunstancias y limitaciones bajo las cuales las fuerzas del ejército iniciarán y/o continuarán comprometiéndose en combates con otras fuerzas oponentes.

RITMO OPERACIONAL .- El paso de una opn u opns, que incluye todas las actividades que la unidad está conduciendo, pudiendo ser una actividad única o una serie de opns.

RIESGO.- Una opción u oportunidad de peligro o malas consecuencias; expuesta a una ocasión de lesión o perdida. El nivel de riesgo está expresado en términos de probabilidad o severidad del peligro.

- S -

SEGURIDAD DE LA INFORMACION.- La protección contra el acceso no autorizado o modificación de la información; durante el almacenaje, procesamiento o tránsito; y contra la denegación de servicio a usuarios autorizados o la provisión de servicio a usuarios no-autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y contrarrestar tales amenazas.

SEGURIDAD DE LAS OPERACIONES (SEGOPE).- Es el proceso de identificar info crítica y consecuentemente analizar las acciones amigas que conllevan las opns militares y otras actividades relacionadas para: (1) Identificar aquellas acciones que pueden ser observadas por los sistemas de inteligencia adversarios. (2) Determinar indicadores de sistemas de inteligencia enos que podrían obtener aquello que puedan interpretar o integrar, derivando info crítica oportuna que sería útil al adversario. (3) Seleccionar y ejecutar medidas que eliminen o reduzcan, a un nivel aceptable, las vulnerabilidades de las acciones amigas a la explotación ena. También se puede definir como, todas las medidas que se toman para mantener la seguridad de Telemática y la seguridad de la info. También envuelve la identificación y eliminación o control de indicadores que puedan ser explotados por organizaciones de inteligencia hostiles o enas.

SEGURIDAD DE SISTEMAS DE INFORMACION (SSI).- Una composición de medios para proteger los sistemas de telecomunicaciones y los sistemas de información automatizados; y la información que trasmiten y/o procesan.

SISTEMAS DE INFORMACION.- La estructura total, organización, personal y componentes que reúnen, procesan, almacenan, trasmitan, muestran, proyectan, difunden y actúan sobre la información.

SISTEMAS OPERACIONALES DEL CAMPO DE BATALLA (SOC´s).- Una lista de actividades tácticas críticas. Los SOC´s proporcionan medios de revisión, de preparaciones o de ejecución de opns en sub-conjuntos abstractos pero interrelacionados. Lo crítico de esta revisión es la sincronización y coordinación de actividades no sólo dentro de un SOC, sino entre varios SOC´s. Los SOC´s incluyen: maniobra, apoyo de fgos, defensa aérea, cmdo de batalla, inteligencia, GE, apoyo administrativo (básicamente logístico), movilidad y supervivencia; sin embargo estas actividades no direccionan tiempo, ritmo, reconocimiento, OI y tácticas.

SISTEMA DE COMANDO Y CONTROL (S-C^2).- Es la combinación de personal, equipo, comunicaciones, computadoras, facilidades, instalaciones y procedimientos empleados por un cmdte en el planeamiento, dirección, coordinación y control de las fuerzas y opns en el cumplimiento de la misión. Las funciones básicas de un S-C^2 son dar sentido válido a la info sobre los eventos y el ambiente, reportes de info, evaluación de la situación y alternativas asociadas para la acción; decidiendo sobre una forma de acción apropiada y ordenando acciones en correspondencia con al decisión.

SEGURIDAD DE COMUNICACIONES (SEGCOM).- Es el conjunto de medidas, acciones y/o actividades diseñadas para proteger nuestras telecomunicaciones; fundamentalmente negando a personas no-autorizadas información de valor que podría derivarse de la posición y estudio de esas telecomunicaciones; o induciendo a error a personas no-autorizadas en su interpretación de los resultados de tal posesión y estudio. La SEGCOM incluye: seguridad física del material de SEGCOM e información, seguridad criptográfica o criptoseguridad, seguridad de trasmisión y seguridad de emisión.

SEGURIDAD DE COMPUTADOR.- Es el conjunto de medidas y controles que aseguran confidencialidad, integridad y disponibilidad de la info procesada y almacenada por un computador; esto incluye políticas, procedimientos y las herramientas de hardware y software necesarias para proteger sistemas de computadoras y la info procesada, almacenada y trasmitida por los sistemas.

SEGURIDAD ELECTRONICA (SEGELEC).- Es la parte de la seguridad de Telemática (SEGOPE) que envuelve un conjunto de medida y/o actividades, diseñadas para proteger o negar a personas no-autorizadas, info de valor que podría derivarse de la interceptación y estudio de radiación electromagnética de no-comunicaciones (radares por ejemplo).

- T -

TAREA TACTICA.- La actividad específica realizada por una unidad mientras conduce una forma de opn táctica o una forma de maniobra. Es el efecto esencial mínimo para cumplir el propósito.

- U -

UNIDAD DE ESFUERZO.- Es la coordinación y cooperación entre todas las fuerzas, no necesariamente parte de la misma estructura de comando, orientada hacia un objetivo comúnmente reconocido.

- V -

VISUALIZACIÓN DEL CAMPO DE BATALLA.- Es el proceso según el cual el cmdte desarrolla un claro entendimiento de su estado o situación actual con relación al eno y el medio ambiente (clima y terreno) prevé un estado final deseado; y luego subsecuentemente visualiza la secuencia de actividades que moverán su fza desde su estado actual a ese estado final. El cmdte articula una visión del campo de batalla a través de la expresión de su intención que guía el desarrollo de un concepto para la opn y la subsiguiente ejecución de la misión.

ANEXO 06: ABREVIATURAS DE TERMINOS RELACIONADOS A LAS OPNS DE INFO

1.	**AC**	**Asuntos Civiles**
2.	AE	Ataque electrónico
3.	AGE	Apoyo de Guerra Electrónica
4.	AIG	Ambiente de información global
5.	AIM	Ambiente de información militar
6.	Apy	Apoyo
7.	Atq´	Ataque
8.	Atq´-C^2	Ataque de comando y control
9.	CAF	Coordinador de apoyo de juegos
10.	C^2	Comando y control
11.	C^3	Comando, control y comunicaciones
12.	C^4 I	Comando, Control, Comunicaciones, Computación e Inteligencia
13.	Cbte	Combate
14.	CCMM	Condiciones meteorológicas
15.	CCR	Cuadro común relevante
16.	CMC^3	Contramedidas de comando, control y comunicaciones
17.	Cmdo	Comando
18.	Cmdos	Comandos
19.	Cmdte	Comandante
20.	Cmdtes	Comandantes
21.	EAGIT	Elemento de actividad de guerra de la información del componente terrestre.
22.	EDB	Evaluación de daños de batalla
23.	EEIA	Elementos esenciales de información amiga
24.	EEMM	Estados mayores
25.	Elón	Escalón
26.	EMBOI	Estado mayor de batalla de las opns de info
27.	**EM**	**Estado Mayor**
28.	Eno (a)	Enemigo (a)
29.	F/A	Forma de acción
30.	FF/A	Formas de acción
31.	Fgo	Fuego
32.	Fza	Fuerza
33.	Fzas	Fuerzas
34.	G – I	Guerra de información
35.	G-C^2	Guerra de comando y control
36.	GE	Guerra electrónica
37.	GFH	Grupo fecha-hora
38.	Gpo	Grupo
39.	GPS	Global Position System (Sistema de posicionamiento global)
40.	IID	Infraestructura de información de defensa
41.	IIG	Infraestructura de información global
42.	IIN	Infraestructura de información nacional

43.	**Info**	**Información**
44.	Infos	Informaciones
45.	IRI	Información relevante e inteligencia
46.	ME	Manual del Ejército
47.	METT-T	Misión, enemigo, terreno – clima, tropas y tiempo
48.	**NICC**	**Necesidades de información crítica del comandante**
49.	NIFA	Necesidades de información de las fuerzas amigas
50.	NPI	Necesidades prioritarias de inteligencia
51.	O/O	Orden de operaciones
52.	OI	Operaciones de información
53.	ONG	Organización no-gubernamental
54.	Opns	Operaciones
55.	Opns/Sicolo	Operaciones sicológicas
56.	OPV	Organización privada de voluntarios
57.	OR&V	Operaciones de reconocimiento y vigilancia
58.	PC	Puesto de Comando
59.	P/O	Plan de operaciones
60.	PIC	Preparación de Inteligencia del Campo de batalla
61.	POV´s	Procedimientos operativos vigentes
62.	Prot-C^2	Protección de comando y control
63.	R&V	Reconocimiento y vigilancia
64.	RP	Relaciones Públicas
65.	RSI	Red del sistema de información
66.	RSID	Red del sistema de información de defensa
67.	Rva	Reserva
68.	SEG/COM	Seguridad de comunicaciones
69.	SEGINFOR	Seguridad de la información
70.	SEGOPE	Seguridad de las operaciones
71.	SINFOR	Sistemas de información
72.	SOC	Sistema Operacional del campo de batalla
73.	Sup	Superior
74.	TO	Teatro de operaciones
75.	TTP´s	Tácticas, Técnicas y Procedimientos
76.	Z/O	Zona de operaciones