ARMADA DEL ECUADOR
ACADEMIA DE GUERRA NAVAL
Guayaquil
-o-

LECTURA RECOMENDADA

El Campo de Batalla Digital

AUTOR: Pedro Jarpa Martínez

Lectura recomendada por:

CPNV (SP) Javier Paredes
Docente de la Academia de Guerra

2022

MOTIVACIÓN A LA LECTURA

Su autor es el distinguido ingeniero Pedro Jarpa Martínez, Ingeniero Politécnico Militar en la especialidad de electrónica, quien ostenta una brillante trayectoria profesional y académica.

El desarrolla un ensayo que está dirigido a aquellos quienes están por iniciarse en el estudio de la guerra electrónica, a aquellos que inician una capacitación para ser usuarios u operadores de sensores o sistemas de guerra electrónica y a quienes serán responsables de su mantenimiento y administración.

Sin, embargo es una lectura que puede servir a todos los que estamos interesados en la guerra electrónica del Siglo XXI.

De esta obra, recomiendo la lectura del Capítulo I "El Campo de Batalla Digital." Especialmente, porque nos permite comprender el porqué la Guerra Electrónica es parte de las Operaciones de Información. Claramente explica: "La revolución tecnológica más significante en la guerra y en la vida actual está en el rol de la información y el conocimiento, y en particular en el grado de la alerta situacional que se le presenta a los comandantes, gracias al incrementado número de sistemas de comunicaciones e información que apoyan a las fuerzas de combate.

Nos va llevando de la mano para entender el arte del mando y la ciencia del control, de los sistemas de mando y control, y de como estos influyen en el ciclo de toma de decisiones.

De como se organiza la guerra electrónica moderna, de acuerdo a los efectos que se puede obtener y de la gestión del espectro electromagnético. Para concluir que: "Los sistemas de mando y control cada día dependen más fuertemente de sistemas de comunicaciones y de información, los que no pueden operar sin el acceso al EEM. Entonces, mientras la revolución de la información promete entregar enormes mejoras a las capacidades de los comandantes, también crea nuevas y potenciales vulnerabilidades. Esas nuevas vulnerabilidades ofrecen nuevas oportunidades para la aplicación de la GE en el campo de batalla."

Inscripción Registro de Propiedad Intelectual Nº 198.320.

https://www.ejercito.cl/descargas/mobile/Njg2

Revista de Marina Año CXXXV, Volumen 137, Número 976.

El mando y control ¿Un arte perdido?

By MC INTYRE ASTORGA, RONALD .

ESCENARIOS DE ACTUALIDAD

- **PUBLISHED AT:** 01/07/2020. VISTO 140 VECES.
- **KEYWORDS (SPANISH):** MANDO Y CONTROL, PLANIFICACIÓN, CONDUCCIÓN OPERACIONAL, MOC.

La experiencia en operaciones, tanto en el país como en el extranjero, hace evidente la necesidad de recuperar el verdadero significado del arte de mado y control. La Academia de Guerra Naval ha tomado el liderazgo en el desafío de mejorar las competencias de planificación y conducción operacional, para lo cual se ha creado el Departamento de Planificación y Conducción Operacional, el cual estará a cargo de apoyar la creación de la doctrina y el procedimiento de planificación y conducción.

El verdadero significado de mando y control se ha perdido con el paso del tiempo, confundiéndose con términos técnicos alejados de su verdadero sentido. Es fundamental que

Capítulo I
El Campo de Batalla Digital

A principios de los años 70, la introducción de las armas de precisión y las capacidades de los computadores produjo la última revolución que cambió el carácter y la conducción de la guerra. Esa fue una revolución centrada en la información sobre el concepto de que el factor dominante en la guerra es la habilidad para reunir, analizar, diseminar y actuar sobre la información del campo de batalla [1].

Los avances en tecnología han producido un ambiente en el campo de batalla moderno que se caracteriza por poseer algunas características como veinticuatro horas continuas de operación; un fuego incrementado en volumen, letalidad, rango y precisión; unidades más efectivas y pequeñas debido a una mejor integración de la tecnología; una disyunción entre una gran dispersión de unidades más móviles, rápidas y una tendencia incrementada por áreas de combate reducidas y congestionadas de fuerzas que se enfrentan; y una marcada dicotomía entre mayor invisibilidad, debido a la dispersión y velocidad y un riesgo incrementado de detección, debido a un número mayor de sensores de mayor capacidad.

La revolución tecnológica más significante en la guerra y en la vida actual está en el rol de la información y el conocimiento, y en particular en el grado de la alerta situacional que se le presenta a los comandantes, gracias al incrementado número de sistemas de comunicaciones e información que apoyan a las fuerzas de combate. Sin embargo, no todos los ejércitos están capacitados para tomar ventaja de esta revolución; en la "era de la información" actual los ejércitos deben estar preparados para enfrentar un amplio espectro de amenazas inherentes a esta era.

La era de la información, con la asociación de las tecnologías de la información, favorece a las redes más que a las jerarquías; difunde y

redistribuye el poder; cruza y redibuja fronteras físicas y responsabilidades y expande horizontes. Esto es particularmente verdadero en el ambiente civil, donde las organizaciones han llegado a ser más democráticas en la distribución de la información y han logrado una mejor eficiencia.

Para la guerra, la mayor lección del mundo comercial es que el conflicto de la "era de la información" es acerca del conocimiento y la habilidad de las redes y de las organizaciones en red, para proveer una mayor ventaja o la superioridad definitiva en el conflicto. Sin embargo, los comandantes militares tienden a ver el mando y la información (incluso las comunicaciones en muchos ejércitos), según las mismas líneas jerárquicas o de mando. En un modelo en red no jerárquico, el flujo de mando y de información debe ser necesariamente divergente. Los sensores, los comandantes y los sistemas de armas están conectados por una grilla en red que asegura que la data de alerta situacional puede ser compartida por todos los elementos, sin importar si pertenecen a la misma unidad. Las líneas de mando no necesitan ser compartidas con los flujos de información. La información se comparte a través de la red; el mando y el control son dirigidos de acuerdo con el orden de batalla preestablecido. Por lo tanto, la adopción de estas tecnologías no afecta solamente la manera en que los ejércitos son dirigidos y controlados, sino que también deben cambiar la forma en que estos son organizados, entrenados y dirigidos.

Entendiendo que las operaciones de guerra electrónica (GE) en el campo de batalla son las operaciones que se realizan a través del espectro electromagnético (EEM), un componente clave del dominio total del espectro es la "superioridad de la información", definido formalmente como la capacidad de recolectar, procesar y diseminar un flujo ininterrumpido de información mientras se explota o niega la habilidad de un adversario para hacer lo mismo. La superioridad de la información puede entonces ser definida como *"aquel grado de supremacía en el dominio de la información que permite la conducción de las operaciones sin una oposición efectiva"*. De este modo, la superioridad de la información se convierte en conocimiento superior que combinado con una doctrina organizacional, entrenamiento, experiencia y un apropiado mecanismo y herramientas de mando y control, alcanza la superioridad en la toma de decisiones.

Las operaciones de información entendidas como aquellas acciones tomadas para afectar la información y los sistemas de información de un adversario mientras se defiende la información y los sistemas de información propios, son un elemento esencial para alcanzar el dominio del EEM. Este tema es el fondo del presente ensayo, ya que la guerra electrónica (GE) es un componente importante de las operaciones de información.

Tal vez el impacto mayor de las tecnologías de la información se encuentra en el concepto emergente de guerra centrada en redes (*network-centric warfare,* NCW). En el concepto antiguo de guerra centrada en la plataforma, la capacidad de detectar y atacar residía normalmente en el mismo sistema de armas *("shooter")* y existía solo una capacidad limitada del sistema de armas para enfrentar blancos debido a que solo podía utilizar la alerta situacional generada por su propio sensor. Si un arma es capaz de enfrentar a un blanco localizado por un sensor remoto, el paso de la data normalmente es vía, un ducto de un sistema de comunicaciones (que conectan un arma directo a un sensor). Opuestamente, en la guerra centrada en redes, los sistemas de armas y los sensores están conectados por redes desplegadas a través de las cuales las armas pueden enfrentar blancos basándose en la alerta situacional que es compartida con otras plataformas. De tal forma se puede aplicar una capacidad de combate con menos sistemas de armas que con los que son normalmente requeridos. El hecho de que los sistemas de armas estén interconectados, no significa que los blancos puedan ser enfrentados aleatoriamente o sin una autorización; el control todavía es esencial para asegurar que los blancos sean atacados de acuerdo con el plan operacional.

Aunque puede continuar existiendo algún rol para los enlaces directos desde los sensores hacia los sistemas de armas, el objetivo final de la NCW es que el empleo de las armas de precisión se basa en información. Ningún sensor por sí solo tiene la capacidad de dirigir las aplicaciones de las armas de precisión, la data debe ser integrada desde un número de sensores y bases de datos, de tal forma que en el campo de batalla moderno, las redes se transforman en un multiplicador de fuerza considerable. Bajo esta condición, los comandantes se encuentran desencadenados gracias a las comunicaciones y no se ven forzados a permanecer en los centro de información (puestos de comando y control). La red de información debe estar presente a tra-

vés del campo de batalla y debe ser fluida, flexible, robusta, redundante y en tiempo real, tener integridad y seguridad, tener capacidad y accesibilidad, ser conjunta y capaz de apoyar una coalición.

La NCW se define como un concepto de operaciones que permite la superioridad de la información, genera un poder de combate incrementado por la interconexión de sensores, quienes toman decisiones y sistemas de armas para alcanzar una alerta situacional compartida, una mayor velocidad de las órdenes, alto ritmo de las operaciones, mayor letalidad, supervivencia incrementada y un grado de autosincronización [1].

La Figura 1.1 ilustra los tres cuadros interconectados de la NCW (el cuadro de la información, el cuadro de sensores y el cuadro de enfrentamiento o enganche) y los tres tipos de participantes (sensores, elementos de comando y armas). El cuadro de información provee la infraestructura a través de la cual la información es recibida, procesada, transportada, almacenada y protegida. El cuadro de sensores contiene todos los sensores, sean estos dispositivos especializados montados en sistemas de armas, portados por soldados individuales o empotrados en equipamiento desplegado. El cuadro de enfrentamiento consiste en todos los sistema de armas disponibles que han sido asignados para crear el efecto necesario en el campo de batalla. Estos tres cuadros existen en el espacio, aire, tierra, bajo y sobre el mar.

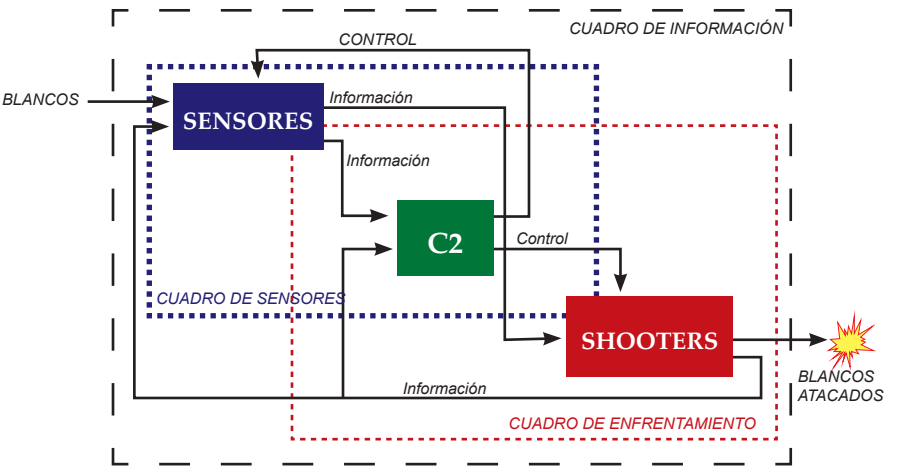

Figura 1.1: Interconexión de los cuadros de la *Network Centric Warfare* (NCW), [1].

El empleo de redes tácticas basadas en enlaces inalámbricos, sin nodos de comunicaciones, tiene la ventaja que las fuerzas pueden dispersarse a requerimiento y aumentar su efectividad rápidamente en tiempo y espacio. De esta forma se tiene menos dependencia de los centros de procesamiento de información, que ahora pueden ser distribuidos para incrementar la supervivencia física sin sacrificar poder de procesamiento.

Este capítulo ya ha entregado una muy pequeña introducción del ambiente operacional. Mientras no se ha considerado en detalle muchos de los aspectos asociados con el impacto significativo que la revolución de la información tiene en los sistemas de armas del campo de batalla, el efecto más significativo para este ensayo de guerra electrónica se encuentra en la habilidad de un comandante para adquirir información, preparar y diseminar planes y luego controlar su ejecución. Este es el negocio del mando y control, que ha llegado a ser altamente dependiente de las comunicaciones protegidas y seguras, así como de sistemas de información efectivos. Por lo tanto, antes de considerar aún más el rol de la guerra de la información, particularmente el rol de la guerra electrónica, es importante abordar el tema del mando y control en más detalle.

Mando y Control (C2)

El mando y control en sí es un concepto muy amplio para ser tratado en detalle por un ensayo. Sin embargo, se puede entender el mando como la autoridad investida en un individuo para la dirección, coordinación y control de las fuerzas militares. El control es el medio por el cual el mando se ejecuta. En una organización simple, el comandante realiza la mayoría del control, pero en una organización más compleja la mayoría de las funciones de control son delegadas a personal de apoyo quienes conforman un cuartel general en apoyo al comandante. El control involucra análisis de requerimientos, asignación de recursos, integración de esfuerzos, dirección, coordinación y monitoreo.

Los dos términos, mando y control, están intrínsecamente entrelazados. El mando no tiene sentido sin la capacidad de controlar y el control no tiene ascendiente sin la autoridad del mando. Por lo tanto, la función de un comandante es comúnmente señalada como comando

y control (C2), que puede ser descrito como el proceso y los medios requeridos para el ejercicio de la autoridad de un comandante sobre las fuerzas asignadas en el cumplimiento de la misión del comandante. Entonces se debe entender que las funciones de comando y control son desarrolladas a través de un concierto de personal, equipamiento, comunicaciones, instalaciones y procedimientos empleados por un comandante con el fin de planificar, dirigir, coordinar y controlar fuerzas y operaciones en el cumplimiento de la misión.

El Ciclo C2

La interdependencia de varios elementos de un sistema de comando y control se ilustra en el ciclo C2 de la Figura 1.2. Aunque es un modelo muy simple, el ciclo C2 es un mecanismo útil para desarrollar una estructura de trabajo para la aplicación del C2 a cualquier nivel. Aquí también es útil visualizar el impacto que los sistemas de información y comunicaciones tienen en el campo de batalla moderno.

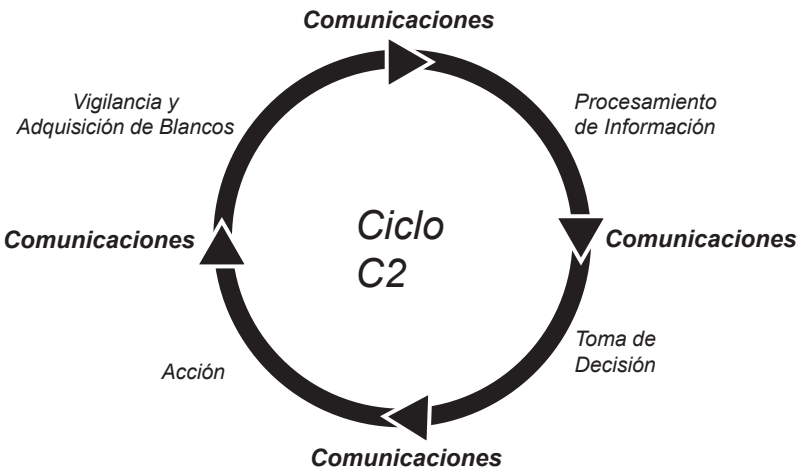

Figura 1.2: El Ciclo de Mando y Control (C2) [1].

El ciclo C2 también es llamado el ciclo de decisión, el *loop* OODA (siglas en ingles de los conceptos de observación, orientación o entendimiento, decisión y acción), o el ciclo de Boyd (coronel retirado de la Fuerza Aérea de Estados Unidos que propuso este concepto). Aunque el ciclo es continuo, se asume que se inicia con la función de

vigilancia y adquisición de blancos u observación, instancia desde la cual los comandantes reciben una amplia gama de información desde muchos sensores y sistemas desplegados. Esa información es invariablemente enviada en forma digital y el rápido incremento del número de sensores y sistemas de vigilancia es predominantemente responsable por la explosión en los requerimientos de transmisión de información digital principalmente inalámbrico en el campo de batalla moderno. Debe considerarse que la data de vigilancia llegará al comandante solo si los sistemas de comunicaciones activos están disponibles para transportar esa información desde los sensores hasta las instalaciones de procesamiento de data en el puesto de mando.

El volumen de información de los sensores que llega al cuartel general es agobiante y debe ser filtrado para luego ser desplegado en un formato apropiado para el comandante y su personal, para proceder con el análisis pertinente y luego con la toma de decisiones. A medida de que el volumen de información crece, la automatización de ese proceso es esencial. En un cuartel general se debe contar con redes de alta velocidad para facilitar el procesamiento de la data que llega en forma continua e ininterrumpida. El comandante entonces debe tomar un número de decisiones a fin con la misión, para luego estructurar y dar cumplimiento a un plan de operación, seguido de órdenes que son transmitidas a las unidades subordinadas a través de redes de voz y data.

El propósito de las etapas del ciclo mencionadas anteriormente, es iniciar la acción. Existen muchos modelos más para mando y control. Sin embargo, el ciclo C2 es adecuado para este propósito, ya que es evidente desde este simple modelo que la habilidad de moverse a través del ciclo C2 más rápido que el adversario es un factor mayor de éxito en el campo de batalla. Es aquí donde la revolución de la información ofrece las mayores ventajas y mejoras, aunque con un correspondiente aumento en vulnerabilidades y el ciclo C2 demuestra una alta dependencia de las tecnologías que requieren el uso del EEM.

El término “digitalización del campo de batalla” se refiere a la automatización a través de redes y procesos digitales de las operaciones de mando y control a través de todo el ámbito del espacio de batalla. Esta integración de nodos terrestres, aéreos y marítimos (nodos de

sensores, de comunicaciones, de mando y de sistemas de armas) en redes digitales continuas, requiere un intercambio digital compatible de data y situaciones operativas comunes a todos los nodos. La seguridad, compatibilidad e interoperabilidad son factores dominantes de conducción hacia la digitalización total a través de todo el espacio de batalla.

Sistemas de Mando y Control

Existen muchas variaciones del término C2 referidas al proceso de ejercer el mando. A partir de este concepto se han desarrollado muchas variantes en su terminología, por ejemplo: comando, control y comunicaciones (C3); sistemas de comunicaciones e información (CIS); comando, control, comunicaciones e inteligencia (C3I); comando, control, comunicaciones, computadores e inteligencia (C4I); comando, control, comunicaciones, computadores, inteligencia, vigilancia y reconocimiento (C4ISR); o comando, control, comunicaciones, computadores, inteligencia, vigilancia, adquisición de blancos y reconocimiento (C4ISTAR). Cada uno de estos términos se justifica por su énfasis sobre elementos particularmente vitales en el proceso de mando y control. Por ejemplo, sin vigilancia y reconocimiento los comandantes están ciegos; sin comunicaciones ellos están aislados y así se pueden encontrar otras acepciones. En términos generales se debe considerar el ciclo C2 como el concepto general que abarca toda la terminología expuesta y que reúne a todos los sistemas que apoyan el término genérico de sistemas de mando.

Para ser exitoso en el campo de batalla moderno un comandante y su personal de apoyo deben ser capaces de moverse a través del ciclo C2 más rápido que cualquier adversario. El éxito en la guerra moderna depende del ritmo de las operaciones, de la letalidad de los sistemas de armas y de la supervivencia de todo el sistema en su conjunto. Los sistemas de mando deben ser ágiles y sensibles a los cambios en las amenazas y deben estar dispuestos a enfrentar una gran cantidad de información de inteligencia y sistemas de vigilancia, ambos de nivel táctico y operativo. En los conflictos recientes, esto ha sobrecargado los sistemas de comunicaciones tácticas como así también ha intensificado los procesos de inteligencia, haciendo extremadamente difícil para el comandante procesar y analizar la información de una manera oportuna.

Un sistema de mando comprende procedimientos manuales y automatizados para apoyar a un comandante y su personal. Los componentes esenciales de un sistema de mando son el comandante, el personal de apoyo, la doctrina y procedimientos, el reconocimiento y los sistemas de vigilancia y adquisición de blancos (STA), los sistemas de comunicaciones y los sistemas de información. Así el componente más importante todavía es el elemento humano que comprende un comandante capaz apoyado por personal bien entrenado y una doctrina apropiada y procedimientos. Aunque se cuente con la enorme ventaja de estar a la par con la revolución de la información, se debe continuar siendo consciente que la tecnología por sí sola no ganará batallas, tampoco la adopción de nuevas tecnologías obviarán la necesidad de desarrollar una doctrina apropiada y los procedimientos correspondientes. Algunas veces los procedimientos demuestran ser más apropiados y su implementación pueden conducir a la supervivencia por sobre la destrucción o degradación de los sistemas de comunicaciones e información. Aunque sea vital actualizarse permanentemente y mantenerse a la par del desarrollo tecnológico, la mayoría de las fallas que han presentado los sistemas de mando y control de este siglo han sido el resultado de errores humanos en vez de fallas de tecnologías. Las Fuerzas Armadas occidentales modernas parecen creer que la precisión en las maniobras se alcanza con la información y un apoyo tecnológico de punta, cuya combinación crearía una agobiante ventaja sobre el adversario. Sin embargo, se debe tener presente ejemplos tan fuertes como los problemas que tuvo EE.UU. en Afganistán, que a pesar de mantener una ventaja tecnológica y un poder aéreo considerablemente superior, no pudo asegurar el éxito en sus campañas.

Finalmente, la implementación de sistemas de información y la tecnología de la información son esenciales para entregar la automatización necesaria para transferir, procesar y almacenar grandes volúmenes de data en el campo de batalla futuro. El desarrollo de la tecnología jugará un rol significativo en el apoyo a los comandantes para permitirles planificar y maniobrar más rápido que sus adversarios. Los sistemas de información y las tecnologías en los próximos años incrementarán considerablemente el alcance, volumen, exactitud y velocidad de la información disponible para la toma de decisiones (función del comandante).

Guerra de la Información

Con la "era de la información" se produce una revolución en las operaciones militares que entrega una ventaja decisiva en el campo de batalla moderno, permitiendo a los comandantes obtener y explotar información de una forma más efectiva, aunque esto tiene su vulnerabilidad. Así como los sistemas de comunicaciones y de información son vitales para la sociedad civil y militar, estos pueden llegar a ser considerados como blancos principales en guerra y también pueden servir como medios principales para conducir operaciones ofensivas. Consecuentemente, la adopción de las tecnologías de la información por parte de los militares crea una nueva vulnerabilidad. La misma tecnología de la información que provee las mayores ventajas para las redes que apoyan a los comandantes modernos, también provee uno de los principales medios para su destrucción, esto porque una alta dependencia de los sistemas de comunicaciones y de información incrementa su vulnerabilidad. Entonces, mientras los sistemas automatizados de comando incrementan la alerta situacional del comandante, estos también pueden volverse contra ellos y ser utilizados para contribuir a su incertidumbre respecto del campo de batalla.

Es evidente que el desplazamiento a través del ciclo de mando y control en el campo de batalla moderno depende fuertemente del empleo del EEM, ya sea para vigilancia y adquisición de blancos, entrega y procesamiento de información o la destrucción de fuerzas adversarias. Esa dependencia es una vulnerabilidad que debe ser explotada al atacar un sistema de mando adversario, mientras se protege el sistema en las fuerzas propias. Las operaciones para contrarrestar el ciclo C2 son denominadas Guerra de la Información, que es un término que involucra un rango de acciones tomadas durante un conflicto para alcanzar la superioridad de la información sobre un adversario y puede ser definido como: "*Acciones tomadas para alcanzar la superioridad de la información afectando la información del adversario, sus procesos basados en información, sus sistemas de información y sus redes basadas en computadores mientras se defiende la información propia, los procesos basados en información, los sistemas de información propios y las redes basadas en computadores" [2].*

El objetivo de la guerra de la información es alcanzar una ventaja significativa en la información que permita el rápido dominio y control de un adversario, incluyendo todas las acciones tomadas para preservar la integridad de los propios sistemas de información ante

la explotación, corrupción o interrupción que el adversario pueda ejercer sobre ellos, mientras que al mismo tiempo se intenta explotar, corromper, interrumpir o destruir los sistemas de información adversarios, así como el proceso de alcanzar una ventaja de información en el empleo de las fuerzas [3]. De esta forma las operaciones de información consideran todos los aspectos vinculados con la forma de obtener la superioridad de la información para apoyar y aumentar los elementos de poder en combate, con el objetivo de dominar el espacio de batalla en el tiempo y lugar correctos y con las armas y recursos adecuados. Las operaciones de información se definen como: operaciones militares continúas en el ambiente de información militar, que permiten aumentar y proteger la habilidad de las fuerzas amigas para recolectar, procesar y actuar sobre información, para alcanzar una ventaja en todo el rango de las operaciones militares. Las operaciones de información incluyen la interacción con el ambiente de información global y la explotación o negación de la información y capacidades de toma de decisión de un adversario [2].

La aplicación de la guerra de la información en las operaciones militares se llama Guerra de Mando y Control (GC2). El objetivo de la GC2 es influir, negar información, degradar o destruir las capacidades de C2 del adversario, mientras se protegen las capacidades C2 propias contra tales acciones. Entonces GC2 comprende dos ramas: ataque C2 y protección C2. Las operaciones de GC2 integran y sincronizan las capacidades de operaciones psicológicas, engaño, seguridad de operaciones, destrucción física y guerra electrónica (GE), todas apoyadas por inteligencia [2]. La componente de GE y en particular su componente de GE de comunicaciones, constituye el interés de este ensayo. Aunque la guerra de la información tiene el potencial de impactar más allá del ambiente táctico, el foco de este ensayo se encuentra en la aplicación de la GE de comunicaciones en el campo de batalla actual.

Guerra Electrónica (GE)

El dominio del espectro electromagnético (EEM) es un componente crucial de la mayoría de las operaciones militares modernas. Existe poco equipamiento en el campo de batalla que no dependa de sistemas de comunicaciones o de información, ahora si nos referimos al ciclo C2, este depende muy fuertemente del EEM para maximizar la efectividad de la vigilancia y la adquisición de blancos, las comunicaciones

y los sistemas de información. Si estos sistemas son destruidos, degradados o engañados, el comandante y su personal no podrán continuar con las operaciones adecuadamente. Por ejemplo, sin comunicaciones el comandante está sordo, mudo y ciego. Por lo tanto, la capacidad de conducir el combate electrónico y dominar el EEM es un componente muy valorado por cualquier estructura de fuerzas moderna.

La GE puede ser definida como el uso del EEM para degradar o destruir la capacidad de combate de un adversario (incluyendo degradar o negar el uso del EEM así como degradar el desempeño del equipamiento adversario, su personal e instalaciones); o proteger las capacidades de combate amigas (incluyendo proteger el uso del EEM por parte de fuerzas propias así como su equipamiento, personal e instalaciones que pueden ser vulnerables a ataques vía el EEM).

El centro de atención está puesto en las comunicaciones y sistemas de información adversarias, por tal razón no se considera el ataque a personal en este ensayo. De igual forma se considera la aplicación de la GE a nivel táctico en el campo de batalla.

La Figura 1.3 ilustra cómo la GE se extiende por sobre todos los aspectos del campo de batalla moderno y tiene el potencial de impactar a todos los elementos del ciclo C2. En resumen, los recursos de la GE son utilizados para monitorear las actividades del adversario en el EEM, indicar su fortaleza y disposición, dar una alerta de sus intenciones, engañar sus sensores e interrumpir su proceso de mando y control, mientras se asegura el uso del EEM para el beneficio de las fuerzas propias.

Figura 1.3: El impacto potencial de la GE sobre el ciclo C2 [1].

Aunque el blanco de la GE es la tecnología, el efecto final recae sobre la habilidad del comandante para moverse a través del ciclo C2. La componente humana del sistema de mando es el enlace más fuerte y a la vez más débil y puede ser rápidamente enceguecido por la acción de la GE adversaria si los sistemas de comunicaciones y de información son interrumpidos, degradados o engañados.

Las actividades de GE son aplicables en toda operación militar. En tiempos de paz se intercepta, localiza e identifica la fuente de una emisión electromagnética potencialmente adversaria. Los análisis posteriores pueden revelar detalles de capacidades así como vulnerabilidades, que pueden ser utilizadas para obtener una ventaja en tiempos de conflicto.

La GE es un área de considerable innovación. Inevitablemente y a menudo las ventajas obtenidas por cambios tecnológicos y de procedimientos, se encuentran con contramedidas igualmente efectivas. Para mantener la ventaja en cualquier conflicto futuro, la información sobre métodos de protección y ataque electrónico de las fuerzas propias debe ser resguardada. Por tal razón, mucha de la data parametrizada asociada con las capacidades de GE es altamente clasificada. Sin embargo, las técnicas fundamentales y las combinaciones factibles pueden ser rápidamente encontradas en publicaciones del tipo fuentes abiertas.

Guerra Electrónica de Comunicaciones y de No Comunicaciones

La GE se divide normalmente en dos áreas principales: GE de comunicaciones y GE de no comunicaciones. La GE de comunicaciones es casi tan antigua como las comunicaciones mismas y en el campo de batalla es mayormente relacionada con las fuentes transmisoras de comunicaciones en las bandas de frecuencias que van desde el HF hasta el SHF. La interceptación y análisis de las transmisiones son usualmente más importantes que los parámetros y/o características del transmisor. La GE de no comunicaciones se ha desarrollado desde el temprano empleo del radar en la Segunda Guerra Mundial y se relaciona principalmente con la protección de las plataformas, orientado específicamente hacia sistemas de radar en bandas como el UHF y superiores. En la GE de no comunicaciones, la medición de las características del emisor es vital, ya que estos son utilizados

para detectar la presencia o posiblemente identificar una plataforma o equipamiento y/o sus capacidades asociadas.

Componentes de la Guerra Electrónica

La GE se divide en tres componentes fundamentales que son aplicables a la GE de comunicaciones y de no comunicaciones, aunque con diferente énfasis:

— **Apoyo Electrónico**, anteriormente denominado medidas de apoyo electrónico (MAE), es la división de la GE que involucra acciones asignadas o bajo el directo control de un comandante operacional para buscar, interceptar, identificar y localizar fuentes de radiación de energía electromagnética intencional y no intencional, con el propósito de lograr el reconocimiento de amenazas inmediatas y la construcción de un orden electrónico de batalla (OEB). Un OEB incluye información sobre la naturaleza y despliegue de todo el equipamiento emisor de energía electromagnética de una fuerza militar incluyendo detalles del equipamiento, frecuencias, modos de operación, localización y otro tipo de data relevante.

– **Ataque Electrónico**, anteriormente denominado contramedidas electrónicas (CME), es la división de la GE que involucra el empleo de la energía electromagnética para atacar personal, instalaciones o equipamiento con la intención de degradar o destruir la capacidad de combate adversaria. El ataque electrónico comprende el *jamming*, el engaño electrónico y la neutralización. El *jamming* es el empleo de la energía electromagnética para evitar que un radiorreceptor reciba señales de interés. El engaño electrónico involucra el empleo de transmisiones falsas o la modificación de las mismas señales adversarias para confundir al adversario. La neutralización describe el empleo de altos niveles de energía electromagnética para interrumpir o dañar permanentemente las capacidades de equipos electrónicos.

– **Protección Electrónica**, anteriormente denominado como medidas de protección electrónica o contra-contra medidas electrónicas (CCME), comprende aquellas acciones tomadas para proteger personal, instalaciones y equipamiento de los efectos del empleo de la GE propia o adversaria que degrade, neutralice o destruya la capacidad de combate propia.

La GE está asociada con la inteligencia de señales (SIGINT, siglas en inglés) que se compone de dos divisiones: la inteligencia de comunicaciones (COMINT) y la inteligencia electrónica (ELINT). COMINT recibe señales de comunicaciones adversarias con el propósito de extraer inteligencia de la información que transportan esas señales. ELINT recibe señales adversarias de no-comunicaciones con el propósito de determinar el detalle de los sistemas electromagnéticos del adversario para desarrollar contramedidas y es por esta razón que los sistemas ELINT normalmente recolectan grandes volúmenes de data sobre vastos períodos en beneficio de lograr un análisis detallado de los sistemas adversarios. Estas dos divisiones reflejan las áreas funcionales de la GE tanto de comunicaciones y de no comunicaciones, pero tienen lugar en un nivel principalmente operativo-estratégico más que en el táctico. El apoyo electrónico por otro lado, se diferencia de SIGINT en el sentido de que recolecta señales enemigas (ya sean de comunicaciones o de no-comunicaciones) con el objeto de alertar su presencia inmediatamente y hacer reaccionar adecuadamente a las señales o los sistemas de armas asociados a esas señales. La señal recibida debe ser interrumpida *(jammed)* o su información de presencia enviada a una capacidad de respuesta letal propia. La señal recibida también puede ser utilizada para levantar una alerta situacional, es decir, identificación y localización de fuerzas adversarias, sistemas de armas o capacidades electromagnéticas. El apoyo electrónico reúne mucha data de señales para apoyar un proceso, haciéndolo menos extenso, con un alto *throughput* (volumen de información que fluye a través de un sistema), para de esta forma determinar solo cuál de los tipos de emisores conocidos están presente y dónde están localizados.

La GE también puede ser categorizada como ofensiva o defensiva. El apoyo electrónico y el ataque electrónico tienden a ser ofensivos, en el sentido que son apuntados contra un adversario e involucran el proceso de búsqueda, interceptación, búsqueda de ubicación (o localización), análisis y comprometer sistemas electrónicos adversarios a través del *jamming*, engaño y neutralización. El dominio de las técnicas ofensivas, capacidades y limitaciones es vital para la conducción efectiva del combate electrónico. La protección electrónica tiende a ser más defensiva y protege el empleo del EEM por parte de las fuerzas propias contra la GE ofensiva de un adversario. La protección electrónica está relacionada con todos los usuarios de equipamiento

electrónico y abarca prácticas tales como la seguridad de emisiones (en inglés, *emission security* - EMSEC) y la seguridad de comunicaciones (en inglés, *comunications security* - COMSEC).

Por otro lado, las técnicas de GE pueden ser caracterizadas como pasivas o activas según su naturaleza. Las actividades pasivas no son detectables y pueden ser implementadas y practicadas en tiempo de paz con un compromiso de riesgo limitado. Las medidas activas son detectables y deben ser cuidadosamente controladas en el campo de batalla y permitidas en tiempo de paz solamente bajo estrictas condiciones de control. El apoyo electrónico tiende a ser pasivo, mientras que el ataque electrónico es activo. La protección electrónica combina ambas medidas, activas y pasivas. El diagrama en la Figura 1.4 entrega una visión de conjunto de las actividades interrelacionadas asociadas con la GE.

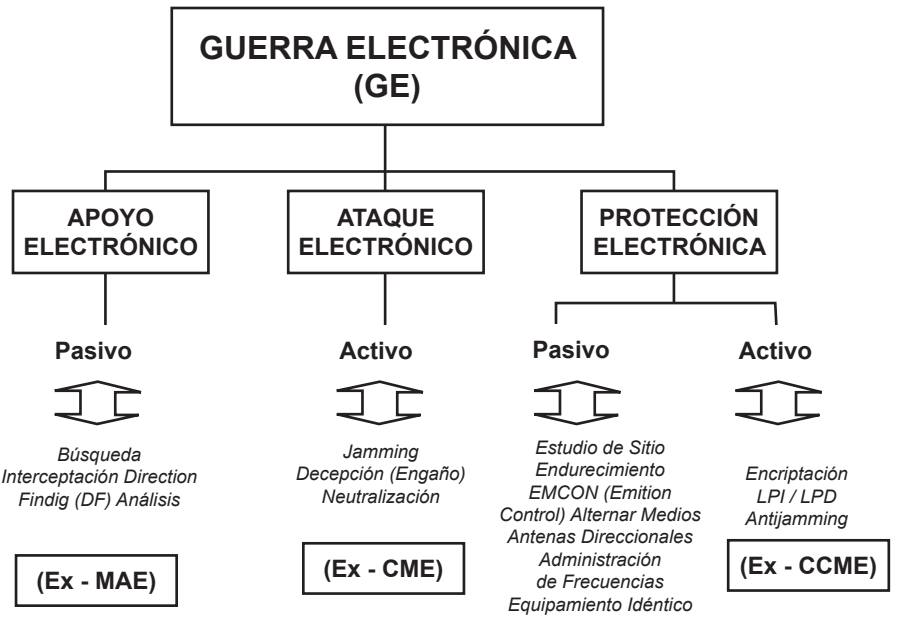

Figura 1.4: Actividades de la GE [1].

El mando y control en la era de la información tiene el potencial de transformar la noche en día, alcanzar espacios de control que pueden ser medidos en términos globales y concentrar el poder de combate sin concentrar fuerzas. De lo anterior sumado a las lecciones de los

conflictos recientes, se ha establecido que lo que puede ser visto puede ser sometido a fuego, por lo tanto impactado y lo que puede ser impactado puede quedar fuera de operación (fuera de combate). La función de ver es mucho más sofisticada actualmente y utiliza sensores electrónicos, ópticos y acústicos que pueden tener cobertura global. Esos sensores pueden ser enlazados en tiempo real a sistemas de armas controlados por computadores, con una exactitud y letalidad sin paralelo. Sin embargo, eso no es suficiente, la ventaja decisiva en el campo de batalla moderno recaerá en el comandante que pueda reunir y explotar la información de una forma los más efectiva posible. Mientras esto es ampliamente asistido por las tecnologías asociadas con la revolución de la información, el elemento humano es finalmente el más significativo y trascendental.

Los sistemas de mando y control cada día dependen más fuertemente de sistemas de comunicaciones y de información, los que no pueden operar sin el acceso al EEM. Entonces, mientras la revolución de la información promete entregar enormes mejoras a las capacidades de los comandantes, también crea nuevas y potenciales vulnerabilidades. Esas nuevas vulnerabilidades ofrecen nuevas oportunidades para la aplicación de la GE en el campo de batalla. Así entonces, en la medida que los comandantes incrementan su acceso a la información, localizada en cualquier red de su mando y control, ya sea de nivel táctico, operativo o estratégico, ellos también se hacen más vulnerables a las ventajas que la guerra de la información pueda explotar en cualquiera de esos niveles.