La colección de ensayos ACAPOMIL tiene por objeto poner a disposición de los oficiales de Ejército y del público en general, textos que signifiquen un aporte a la discusión académica en temas de ciencia y tecnología para la defensa.

Se espera llenar un vacío en la cultura profesional de todos los interesados en la discusión y reflexión sobre estas materias que representan un gran desafío.

Títulos de la Colección:

1. *De Fantasmas y de Máquinas*
2. *Explosivos, Propelentes y Pirotecnia*
3. *Guerra Electrónica*

En este ensayo, publicado como número 3 de la Colección Academia Politécnica Militar, el ingeniero Pedro Jarpa Martínez describe los principios operacionales de los sistemas de información que soportan los sistemas de mando y control, sus sensores, sus sistemas de armas y las técnicas de protección y ataque electrónico empleadas para destruirlos, degradarlos o neutralizarlos. Estos temas son tratados bajo un criterio académico-operativo y pueden ser de mucha utilidad para los ingenieros, oficiales, especialistas o quienes requieran obtener un entendimiento de la aplicación de la guerra electrónica en el campo de batalla contemporáneo.

Esta obra está dirigida a aquellos alumnos y profesionales que están por iniciarse en el estudio de la guerra electrónica; para los que inician una capacitación para ser usuarios u operadores de sensores o sistemas de guerra electrónica y, finalmente, para quienes serán responsables de su mantenimiento o administración. Su objetivo es proporcionar un modelamiento teórico general, de tal forma que permita un fácil entendimiento para alumnos de ingeniería que hayan aprobado las ciencias básicas. Así el presente ensayo podrá ser leído y comprendido por cualquier persona con un marcado gusto por las ciencias de la ingeniería y un interés en los sistemas de armas, de comunicaciones y sensores utilizados por las Fuerzas Armadas.

Pedro Jarpa Martínez

GUERRA ELECTRÓNICA

3

Pedro Jarpa Martínez
(Ms. Sc.)

GUERRA ELECTRÓNICA

El dominio del espectro electromagnético y las vulnerabilidades de las tecnologías de la información en el campo de batalla digital

Colección Academia Politécnica Militar del Ejército de Chile
ACAPOMIL

BIOGRAFÍA

El ingeniero Pedro Jarpa Martínez nació en Concepción, Chile. Ingresó a la Escuela de Aviación y egresó como oficial de la FACH el año 1990. Se tituló en la Academia Politécnica Aeronáutica como ingeniero (E) en Sistemas de Armas con mención en Telecomunicaciones y posteriormente estudió en la Academia Politécnica Militar recibiendo, en el año 1997, el título de Ingeniero Politécnico Militar en la especialidad de Electrónica.

Sus estudios de posgrado los realizó en la Naval Postgraduate School de Monterey - California, y obtuvo el grado de Master of Science in Electrical Engineering con mención en Joint Services Electronic Warfare, paralelamente obtuvo una certificación como Information Systems Security Professional. En la Escuela de Negocios Española IEDE, obtuvo un MBA.

En la FACH se desempeñó como oficial de telecomunicaciones e informática y ocupó el cargo de jefe de mantenimiento del sistema de alarma temprana aerotransportado, fue operador e instructor de sistemas COMINT y ELINT. Fue jefe del Departamento de Guerra Electrónica de la Dirección de Telecomunicaciones e Informática y posteriormente formó parte del Centro de Guerra Electrónica.

En el año 2009, se unió a la empresa de telecomunicaciones Raylex S.A., como gerente de operaciones. Actualmente es profesor de pre y posgrado en la Academia Politécnica Militar.

GUERRA ELECTRÓNICA

Pedro Jarpa Martínez

ACADEMIA POLITÉCNICA MILITAR
SANTIAGO, 2013

Editor:
Brigadier Víctor Aguilera Acevedo, Investigador del Departamento de Investigación y Desarrollo.

Diseño de la Portada:
Sr. Michel Rippetti Bergoing
Sr. Marcelo Gómez Román

Inscripción Registro de Propiedad Intelectual Nº 198.320.
Impreso en los talleres del Instituto Geográfico Militar, agosto 2013.
300 ejemplares.

Presentación

El presente ensayo, titulado GUERRA ELECTRÓNICA, se suma a la colección de libros del Fondo Editorial de la Academia Politécnica Militar.

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.

En la actualidad, la guerra electrónica es un tema de gran relevancia por la trascendencia que implica el control del espectro electromagnético en apoyo a las operaciones militares, su capacidad de degradar las comunicaciones y sistemas de armas del adversario, reduciendo su ritmo de combate e incrementando el propio.

La guerra ha evolucionado y se pueden distinguir cuatro generaciones:

1) La Guerra de Primera Generación. Se inició con las armas de fuego y la formación de los ejércitos profesionales. Paradigmas de esta guerra son las campañas napoleónicas, las guerras de la independencia de América Latina y la Guerra de Secesión de Estados Unidos de América.

2) La Guerra de Segunda Generación. El elemento fundamental de esta categoría es la mecanización de las fuerzas y la capacidad de transportar un gran número de tropas. Ejemplos: Primera Guerra Mundial y la Guerra del Chaco.

3) La Guerra de Tercera Generación. Se caracteriza por la velocidad y sorpresa de los ataques basado en la superioridad tecnológica de la fuerza. Ejemplos: Guerra relámpago *(Blitzkrieg)* del Ejército

alemán en la Segunda Guerra Mundial, Guerra de Corea y la invasión a Iraq en el año 2003.

4) La Guerra de Cuarta Generación. Se caracteriza por el hecho que las grandes batallas desaparecen casi completamente y aparecen las tácticas militares asimétricas que implican grandes consecuencias en la población civil. Las dimensiones de las fuerzas en conflicto son asimétricas. Ejemplos: Guerra de Vietnam, Guerra de Afganistán, Guerra de guerrillas, Terrorismo y el contraterrorismo. En esta clase de guerra se incrementa cada vez más el rol de la guerra electrónica.

La guerra electrónica preocupa incluso a Estados Unidos de América, considerado el país más poderoso del mundo. En su doctrina de empleo de los medios de defensa, ese país establece un orden de intervención de un teatro de operaciones que se basa en alcanzar la supremacía o control de distintos dominios hasta concretar el dominio total del teatro. Es así que para que las unidades de superficie tomen control del territorio en el que se desarrollan las operaciones, previamente se debe haber alcanzado el dominio del espacio aéreo, es decir, el control de las operaciones aéreas con el objetivo de eliminar cualquier amenaza que por ese medio pudiese agredir a las fuerzas de superficie. Pero previo a alcanzar el dominio del espacio aéreo debe alcanzarse el dominio del espectro electromagnético, con el objetivo de asegurar su empleo en beneficio de las fuerzas propias. Este es el enfoque que se resalta en el texto, es decir, proteger y asegurar los sistemas de comunicaciones que sustentan los sistemas de mando y control, garantizar que los sensores reporten sus detecciones a los escalones superiores de conducción de las operaciones y que los sistemas de armas cumplan su objetivo sin interferencias por parte del adversario.

El libro del ingeniero Pedro Jarpa Martínez, que me honro en presentar, desarrolla en cinco capítulos una visión completa del tema guerra electrónica. Se inicia en su primer capítulo con el tema el campo de batalla digital, continuando con sensores, guerra electrónica de telecomunicaciones, protección electrónica y finaliza con una visión prospectiva en el capítulo titulado el nuevo escenario.

Como lo señala el autor, esta obra está dirigida a todos los alumnos y profesionales que tienen interés por iniciar estudios en la compleja problemática de la guerra electrónica.

La Reina, Invierno de 2013

OSVALDO MAGNA QUEZADA
Coronel
Director de la Academia Politécnica Militar

Índice

Guerra Electrónica

Juppiter Terminus

El dominio del espectro electromagnético y las vulnerabilidades de las tecnologías de la información en el campo de batalla digital.

Pedro Jarpa Martínez

(Ms.Sc.E.E.)

Introducción

La guerra electrónica es la acción militar cuyo objetivo es lograr el dominio del espectro electromagnético. Para lograr este objetivo se requieren acciones ofensivas y defensivas coordinadas, con acciones de apoyo necesarias para proveer inteligencia y reconocimiento de amenazas que permitan la ejecución de las primeras acciones con la mayor eficiencia posible. Básicamente la guerra electrónica es la batalla por el control del espectro electromagnético, sin embargo, se reconoce que la función primaria del espectro es ser un "carrier" o proveedor del transporte de información esencial para cualquier operación militar. Por esto, la guerra electrónica es un componente crítico de lo que se define como guerra de la información, cuya función es negar al enemigo el uso de la información crítica, mientras se protegen los recursos de información propios.

La atrición ya no es el mayor objetivo en las operaciones militares, hoy ha sido reemplazado por la ejecución de ataques quirúrgicos con la finalidad de separar a un comandante de sus fuerzas. Esta acción es definida como guerra de comando y control, donde la guerra electrónica igualmente cumple una función crítica. El conocimiento de la situación actual es otra función de la guerra electrónica de gran trascendencia, que involucra el empleo de receptores que proveen información lo más detallada y completamente posible del campo de batalla a todos los escalones de la conducción militar.

Actualmente es posible realizar operaciones militares tendientes a lograr un objetivo definido por medio del empleo de los medios terrestres, navales o aéreos y los sistemas de armas asociados a estos. Sin embargo, ya no es necesario atacar directamente a las fuerzas adversarias para lograr ese objetivo y más aún, no es necesario destruir un blanco primario o destruir directamente a sus defensas. Esto puede lograrse gracias a la degradación, neutralización total y/o temporal que los sistemas de guerra electrónica pueden ejercer sobre

los sistemas de control de fuego y de mando y control del adversario. De esta forma las operaciones militares se ven favorecidas por el consiguiente ahorro logístico en armamento y la menor exposición de fuerzas propias al fuego adversario al no tener que enfrentarse directamente entre sí.

A pesar de los años de trabajo en mantenimiento de sensores, planificación y operación de sistemas de guerra electrónica, en la evaluación de estos mismos como ingeniero y actualmente como profesor de esta cátedra, el autor se ha percatado que no existe un texto escrito en español y actualizado, que explique las funciones principales de los sistemas de guerra electrónica, sus componentes, las limitaciones de algunos sensores como el radar, de un sistema de control de fuego asociado a un sistema de armas y qué hace efectivo a un sistema integrado de defensa electrónica. Por tal razón, haciendo uso de la experiencia y conocimientos adquiridos como oficial de guerra electrónica en la Fuerza Aérea de Chile, el autor considera que redactar un ensayo que describa los principios operacionales de los sistemas de información que soportan los sistemas de mando y control, sus sensores, sus sistemas de armas y las técnicas de protección y ataque electrónico empleadas para destruirlos, degradarlos o neutralizarlos en el teatro de operaciones bajo un criterio académico-operativo, puede ser de mucha utilidad para aquellos ingenieros, oficiales, especialistas o quienes requieran obtener un entendimiento de la aplicación de la guerra electrónica en el campo de batalla contemporáneo.

El ensayo propuesto 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. La idea es proporcionar un modelamiento teórico general y en la medida de lo posible matemático, de tal forma que permita un fácil entendimiento para alumnos de ingeniería que hayan aprobado las ciencias básicas. Así el presente ensayo podrá ser leído y comprendido por cualquier persona con una educación superior aprobada o con un marcado gusto por las ciencias de la ingeniería y un interés en los sistemas de armas, de comunicaciones y sensores utilizados por las Fuerzas Armadas. A lo largo del ensayo el lector será frecuentemente invitado a consultar las referencias apropiadas para un análisis en profundidad de los temas abordados. En

este sentido el autor cita las publicaciones de reconocidos autores y comparte el pensamiento de varios de ellos, especial reconocimiento recae en quienes tuvo la suerte de conocer y ser su alumno, como es el caso del profesor David Adamy (autor de varios libros de guerra electrónica, profesor del autor en el curso de "Advanced Electronic Warfare"). También el profesor Phillip Pace (profesor guía de la tesis de posgrado del autor, investigador y jefe de proyectos de investigación para el "Naval Research Laboratory" de la USNAVY), el profesor Curtis Schleher (autor de otros libros del área y jefe de proyecto del sistema de alarma temprana aerotransportado "AWACS"), y el profesor David Jenn (autor de libros e investigador en áreas como diseño de antenas, predicción de sección cruzada de radar, electromagnetismo, radar, guerra electrónica y microvehículos aéreos), todos ellos fueron profesores del autor en el "Master of Science in Electrical Engineering", con mención en "Joint Services Electronic Warfare", cursado en la Naval Postgraduate School de Monterey, California.

La guerra electrónica se divide en dos grandes campos de acción, uno es su aplicación en las telecomunicaciones y el otro en los sensores y sistemas de control de fuego asociados a sistemas de armas. En este ensayo se abordará ambas concepciones enfocando sus aplicaciones al ciclo de mando y control, desde los sensores del campo de batalla que por medio de las líneas de comunicaciones transmiten la información (data) obtenida a los centros de mando y control para su procesamiento, análisis y decisión, y cómo esta decisión es transmitida a los sistemas de control de fuego para el empleo y guiado de las armas. Es a través de este proceso que se abordará el empleo de la guerra electrónica para apoyar y proteger electrónicamente el ciclo de mando y control propio e interrumpir el ciclo adversario.

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.

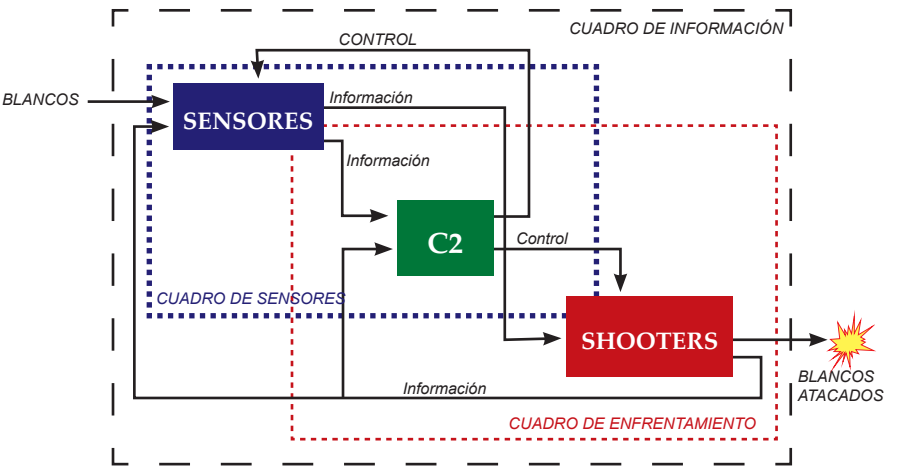

Figura 1.1: Interconexión de los cuadros de la *Network Centric Warfare* (NCW), [1].

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.

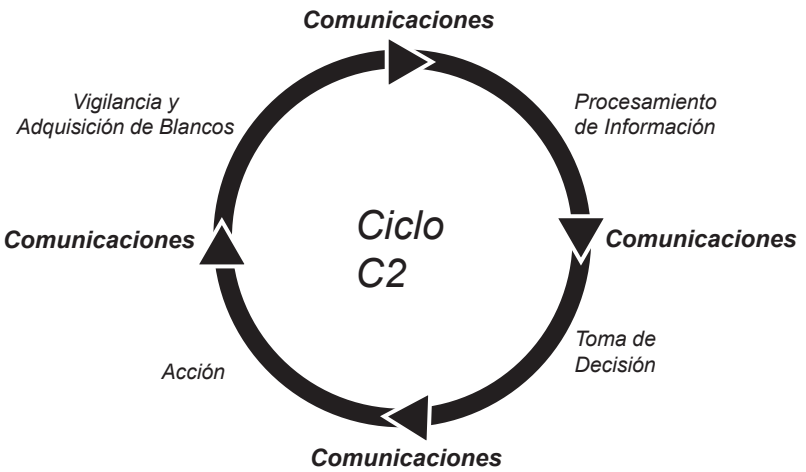

Figura 1.2: El Ciclo de Mando y Control (C2) [1].

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.

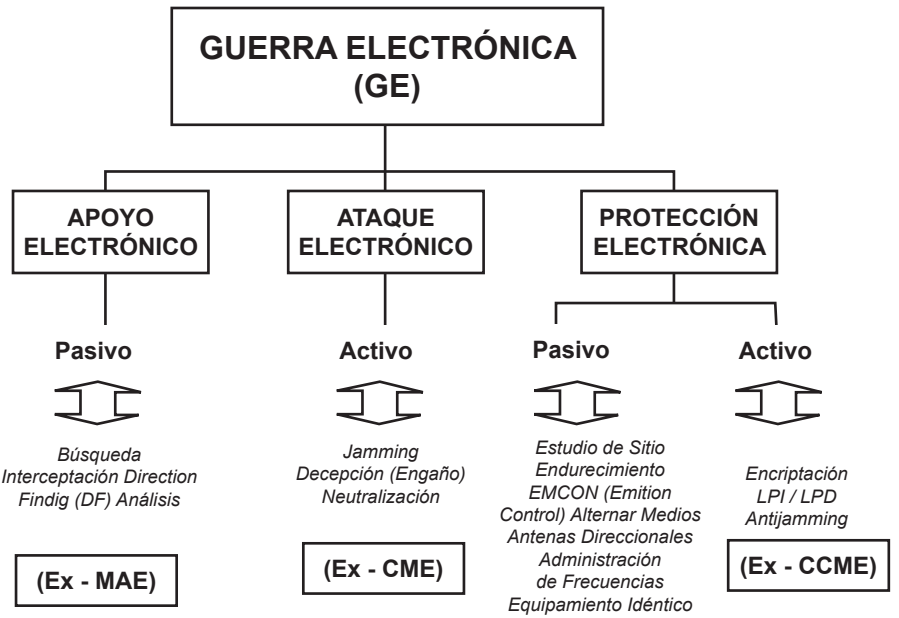

Figura 1.4: Actividades de la GE [1].

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.

Capítulo II

Sensores (Radar - Radio Detección y Rango)

Varios autores sostienen que la llave para entender los principios de la GE es tener un muy buen entendimiento de la teoría de radiopropagación. Si se entiende cómo se propagan las señales de radio, se logrará una progresión lógica para entender cómo ellas son interceptadas, interrumpidas (jammeadas) o protegidas. Sin ese entendimiento resulta muy difícil comprender los conceptos de la GE.

Una vez que se conocen unas fórmulas muy simples, se estará en condiciones de plantear escenarios de GE y poder dar solución a los problemas reales del campo de batalla. Si se llega a ese punto, rápidamente se puede notar cuando alguien trata de quebrar las leyes de la física, como cuando se está frente a representantes de empresas tratando de vender sistemas cuyas capacidades nominales están más cerca de la magia de "Star Wars" que del equipamiento real.

Señales de Radar o Señales de Comunicaciones… ¿Cuál es la amenaza?

Las señales hostiles normalmente se dividen en amenazas de radar o de comunicaciones, pero antes de profundizar en este tema se debe definir qué se entiende por amenaza. Las amenazas son los dispositivos destructivos o sistemas de armas, pero en la GE lo normal es asociar las señales con los sistemas de armas correspondientes, así es que es usual definir amenaza como una *"señal asociada con una amenaza real que potencialmente es un sistema de armas"*. Aunque esto puede ser confuso, es la forma en que los oficiales de GE se refieren al tema.

Entonces se deben diferenciar las señales de radar que son utilizadas para medir localización, distancia y velocidad, mientras que las señales

de comunicaciones transportan información desde un punto a otro. Aunque los dos tipos de señal tienen funciones totalmente diferentes, pueden tener parámetros similares. Las señales de radar pueden ser ondas pulsadas o continuas mientras que las señales de comunicaciones son por naturaleza continuas, excepto por algunos casos especiales. Las señales de radar están en el rango de frecuencia de las microondas, pero pueden llegar a operar en frecuencias tan bajas como la parte alta del VHF y alcanzar el rango de las ondas milimétricas. Las señales de comunicaciones pueden transportar voz, video o solo data y usualmente se encuentran en el rango de frecuencias del HF, VHF y UHF, sin embargo pueden ser encontradas en el rango de las VLF hasta las ondas milimétricas.

Amenazas

La Tabla 2.1 presenta una clasificación de los tipos de amenazas en cuanto a técnicas de guerra electrónica para distintas plataformas. El propósito de esta tabla es mostrar la aplicación de la amenaza que normalmente se espera. Así las armas guiadas por radar son la primera amenaza para aeronaves y buques. La amenaza principal para vehículos de superficie e instalaciones fijas (infraestructura) son las armas guiadas por láser. Los misiles con guía térmica (infrarrojo) son la amenaza principal para las aeronaves.

PLATAFORMA AMENAZADA

TIPO DE AMENAZA	AERONAVES	BUQUES	VEHÍCULOS DE SUPERFICIE	INFRAESTRUCTURA FIJA
Armas guiadas por radar	■	■	◊	○
Armas guiadas por láser	○	◊	■	■
Armas de guiado IR	■	○	◊	○
Comunicaciones letales	■	◊	◊	■

■ Amenaza Primaria ◊ Amenaza Secundaria ○ Normalmente No

Tabla 2.1: Tipos de amenazas para distintas plataformas [3].

Armas Guiadas por Radar (Radares de Control de Fuego)

Según se muestra en la Figura 2.1, un radar es utilizado para localizar blancos y predecir su trayectoria de desplazamiento y un misil es

guiado para interceptar el blanco. Existen cuatro esquemas básicos de guiado que pueden ser aplicados a un sistema de armas guiado por radar. Cada esquema tiene una configuración de radar diferente con sus correspondientes fortalezas y debilidades, asociadas a los tipos de blancos para los cuales son apropiados.

Los buques son los blancos comúnmente más atacados por armas guiadas por radar. Un avión u otra plataforma pueden localizar un buque e identificarlo como blanco. Entonces, un misil es lanzado contra el buque. Usualmente, la plataforma desde la cual es lanzado el misil deja el enfrentamiento, abandonando el área de combate. Cuando el misil se encuentra lo suficientemente cerca del blanco, adquiere al buque por medio de su radar, luego se engancha en este y sigue sus desplazamientos. Finalmente, el misil atacará el buque (blanco) en su línea de flotación o hará un último movimiento vertical para atacar en picada sobre la cubierta del buque.

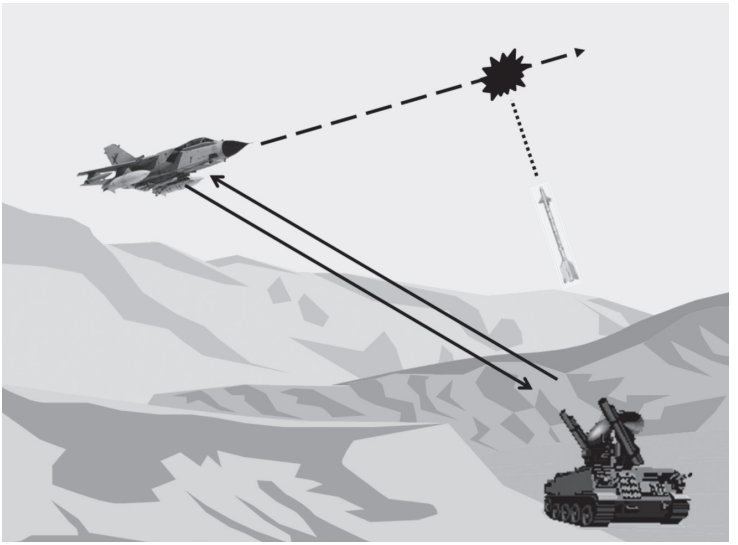

Figura 2.1: Un radar antiaéreo determina la localización y el vector de desplazamiento de un blanco aéreo, para predecir su trayectoria de vuelo y lograr que un misil intercepte esa trayectoria de vuelo. Fuente: elaboración propia.

Armas Guiadas por Láser (Designación del blanco por Láser)

La Figura 2.2 muestra un ataque sobre un blanco móvil terrestre. La misma técnica puede ser utilizada para atacar infraestructura crítica

adversaria, por ejemplo un muelle o un puente. En este tipo de ataque, el láser debe seguir al blanco de tal manera que un misil (que es típicamente lanzado por otra plataforma) se enfoca sobre el destello del láser reflejado sobre la superficie del blanco. La plataforma designadora puede ser una aeronave pilotada o no pilotada (UAV) la que debe mantener la línea vista con el blanco durante todo el ataque.

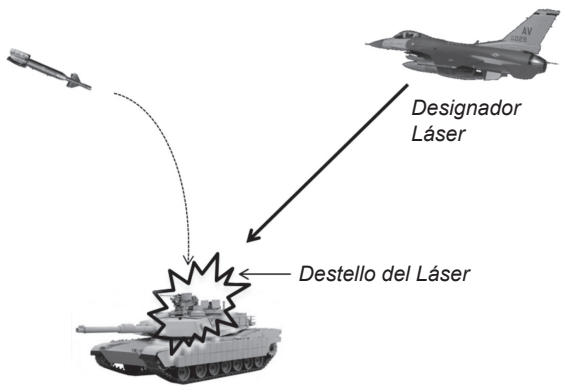

Figura 2.2: Un arma guiada por láser sigue el destello sobre un blanco fijo o móvil que un designador desde otra plataforma ilumina.Fuente: elaboración propia.

Armas Guiadas por Energía Infrarroja (IR)

Todo cuerpo emite algún nivel de energía infrarroja (IR); a mayor temperatura de un objeto, mayor energía emite. Como el motor de un avión jet opera a altas temperaturas, proporciona un blanco muy distintivo para los misiles guiados por calor. Los primeros misiles que atacaban una aeronave se enganchaban en el blanco de alto calor que este representaba. Por tal razón se debe tener presente que las armas pequeñas, hombro-portadas que lanzan misiles IR pueden ser letales para aeronaves en vuelo de bajo nivel. Los misiles IR son utilizados en ataques aire-aire, superficie-aire y aire-superficie. Los sensores de misiles modernos pueden detectar y seguir la energía IR de los blancos a temperaturas considerablemente menores que las de un motor jet.

Comunicaciones Letales

El término comunicaciones letales suena como una contradicción ya que las comunicaciones se refieren a la transferencia de información. Sin embargo, en casi todos los sistemas de armas, la información

acerca de la localización del blanco y la habilidad de guiar un arma hacia el blanco se ubican en lugares distintos. Por tal razón el sensor debe transferir la información a algún tipo de centro coordinador del ataque y ese centro debe transferir la adquisición y/o los comandos de guiado al arma. Así la comunicación que transfiere esa información es extremadamente letal.

A continuación, un ejemplo muy sencillo de comunicaciones letales, según se observa en la Figura 2.3. La artillería ha eliminado más soldados que otro tipo de armas y no puede apuntar a los blancos sin comunicaciones que le provean información de localización. Los cañones harán fuego en una condición sin línea de vista con el blanco, en respuesta a una elevación calculada, resistencia al viento y carga de propulsión, instruidas desde un centro de control de fuego. El centro de control de fuego modifica sus instrucciones a los cañones, en respuesta a la información que llegue desde un observador adelantado que puede ver el blanco y dónde está impactando el fuego de artillería. Ambos recorridos de las comunicaciones son extremadamente letales.

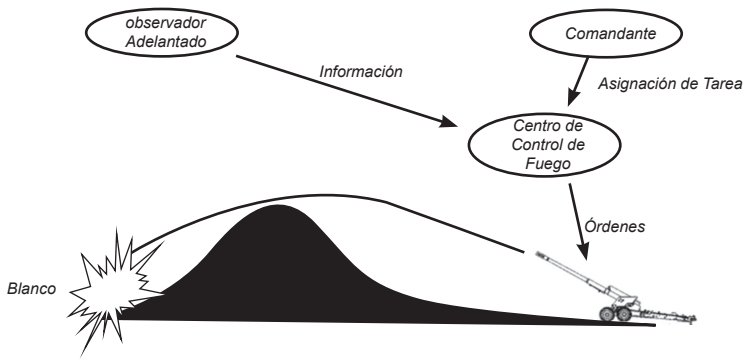

Figura 2.3: El fuego de artillería es ajustado al blanco gracias a comunicaciones consideradas letales entre un observador adelantado y un centro de control de fuego y entre el centro de control de fuego y las armas (cañones).
Fuente: elaboración propia.

Rangos de Frecuencia

La Figura 2.4 muestra los nombre de las bandas de frecuencia en el rango de las amenazas importantes de 1 MHz a 100 GHz. Esta figura tiene tres columnas diferentes, mostrando las tres formas más comunes en que se clasifican los rangos de frecuencia. La columna de la

izquierda muestra la notación científica común, donde esas bandas son divididas en múltiplos de tres. Esto se debe a que cada una cubre un orden de magnitud de longitud de onda. Por ejemplo, el VHF va desde los 30 a los 300 MHz, que corresponde a la longitud de onda desde 1 a 10 metros.

La relación entre la frecuencia y la longitud de onda está dada por la fórmula: $f\lambda = c$, donde f es la frecuencia en Hertz, λ es la longitud de onda en metros y c es la velocidad de la luz en metros por segundo ($3x10^8$ m/s).

La columna de la derecha muestra las bandas de la GE. Las frecuencias de los radares amenaza son descritas en términos de esa designación. Por ejemplo, la banda D cubre desde 1 a 2 GHz. Por otro lado, la columna del centro muestra las bandas oficiales de radar, se debe tener presente que los componentes (antenas, amplificadores, receptores y otros) son clasificados en términos de estas bandas.

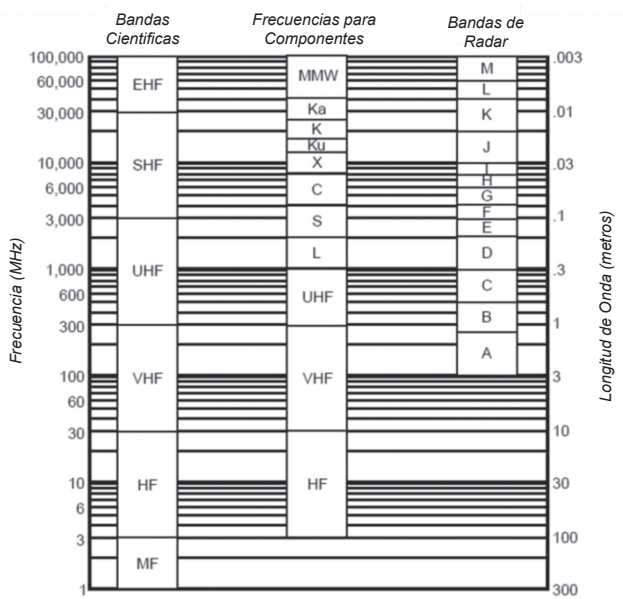

Figura 2.4: Designación de bandas de frecuencia por: bandas científicas, rangos para componentes y bandas de radar [3].

La Tabla 2.2 describe el tipo de actividad por señal que toma lugar en cada rango de frecuencia. Una generalidad acerca de la frecuencia de

una señal es que la transmisión se hace más dependiente de la línea de vista a medida que la frecuencia se incrementa. Las señales HF y de frecuencias más bajas pueden propagarse claramente alrededor de todo el mundo. Las señales VHF y UHF pueden propagarse más allá de la línea de vista, pero están sujetas a una atenuación severa. Las señales de microondas y de ondas milimétricas son usualmente consideradas absolutamente dependientes de la condición de línea de vista.

RANGO DE FRECUENCIA	ABREVIATURA	TIPO DE SEÑAL Y SUS CARACTERíSTICAS
Muy baja, baja y frecuencia media (3 kHz a 3 MHz)	VLF, LF MF	Comunicaciones de largo alcance (buques en el mar). Ondas de superficie que circulan la Tierra. Radio AM Comercial
Alta frecuencia (3 a 30 MHz)	HF	Comunicaciones más allá del horizonte, señales reflejadas desde la ionósfera
Muy alta frecuencia (30 a 300 MHz)	VHF	Comunicaciones móviles, TV y radio FM comercial. Pérdidas severas si no existe línea de vista
Ultra alta frecuencia (300 MHz a 1 GHz)	UHF	Comunicaciones móviles, TV. Pérdidas severas si no existe línea de vista
Microondas (1 a 30 GHz)	μw	TV y enlaces telefónicos, comunicaciones satelitales, radares. Requiere línea de vista
Ondas milimétricas	mmw	Radares, data links. Requiere línea de vista. Alta perdida en lluvia y niebla

Tabla 2.2: Rangos de frecuencia y sus aplicaciones típicas [3].

Una segunda generalidad acerca de las frecuencias es que la cantidad de información transportada por una señal es generalmente proporcional a la frecuencia transmitida. Esto se debe a que la cantidad de información transportada depende del ancho de banda de la señal. Por tal razón, las señales que transportan mucha información (por ejemplo, comunicaciones de banda ancha, televisión o radares) se encuentran en las frecuencias más altas.

Sistemas de Guiado de Armas

Existen cuatro tipos básicos de guiado utilizados por sistemas amenazas. Estos son activo, semiactivo, telecomando y pasivo. El tipo de guiado seleccionado para un sistema amenaza depende de la naturaleza de la plataforma involucrada y de la dinámica del enfrentamiento o ataque.

Guiado Activo

El guiado activo requiere que un radar sea localizado en el arma misma. Los misiles antibuques son una aplicación importante de este tipo de guiado. Una vez que un misil es lanzado, viaja hacia el área general del buque-blanco, enciende su radar, adquiere el blanco y se autoguía a impactar contra el buque. El guiado activo tiene las siguientes ventajas: la plataforma que lanza el misil puede dejar el área inmediatamente después del lanzamiento, el guiado es más exacto a medida que el rango hacia el blanco disminuye y es muy difícil interferirlo a corta distancia (debido a que la potencia del radar sobre el blanco está en función inversa del rango).

Guiado Semiactivo

En el guiado semiactivo (ver Figura 2.5), el arma solo tiene un receptor. El transmisor se encuentra localizado remotamente, por ejemplo, en la plataforma de lanzamiento del arma. El arma entonces busca y sigue la señal reflejada desde el blanco, que se encuentra iluminado por el transmisor de la plataforma de lanzamiento, el que puede ser un radar o un láser. Cuando el medio de guiado es un radar, obedece a una configuración del tipo radar biestático, muy común en misiles superficie-aire. Otro caso importante de guiado semiactivo es el guiado láser que sigue la cintilación de un designador láser. Este tipo de guiado requiere que la plataforma que porta el iluminador permanezca con línea de vista sobre el blanco durante todo el ataque.

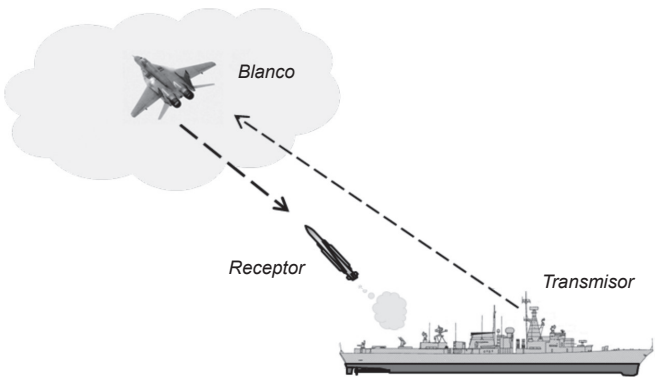

Figura 2.5: El guiado semiactivo involucra un receptor en el arma (misil) y un transmisor remoto. El arma sigue la señal reflejada por el blanco.
Fuente: elaboración propia.

Guiado por Telecomando

En un guiado del tipo telecomando, un sensor (usualmente un radar) sigue un blanco para predecir su trayectoria de desplazamiento. Basado en la información del seguimiento obtenida por el sensor, un arma es guiada hacia un punto futuro en el cual interceptará al blanco (ver Figura 2.6). El arma no tiene información de la localización del blanco, solo se dirige hacia dónde se le instruya a través del telecomando. Uno o más misiles son asignados y dirigidos por un radar de superficie. Las baterías antiaéreas controladas por radar utilizan guiado por telecomando debido a que sus proyectiles son disparados hacia un acimut y ángulo de elevación apropiados, para que con la sincronización justa puedan explosar en una posición futura del avión, operación que obedece a una predicción estimada por el sistema antiaéreo.

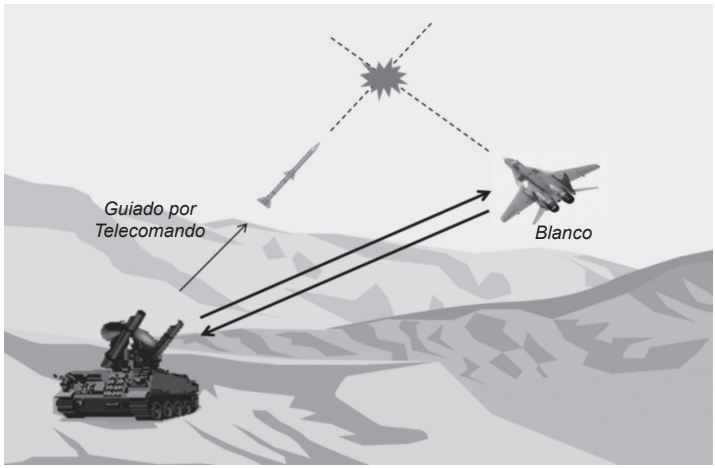

Figura 2.6: En un guiado por telecomando, un radar localiza y sigue al blanco y a la vez guía al arma (misil) a interceptar el blanco. Fuente: elaboración propia.

Guiado Pasivo

Las armas de guiado pasivo siguen alguna señal emitida desde el blanco. Ejemplo: los misiles antirradiación siguen la señal transmitida por un radar y los misiles IR siguen el calor radiado por un blanco (como un avión). En este caso el sistema de armas no emite ningún tipo de señal hacia el blanco. Como los sistemas de guiado activo, el

guiado pasivo permite el lanzamiento de armas del tipo "dispara y olvida". Esto quiere decir que la plataforma de lanzamiento (incluyendo a infantería que utiliza misiles hombro-portados) puede dejar el área del lanzamiento o esconderse tan rápido como el arma sea lanzada.

El Radar

El radar es un sistema electromagnético utilizado para la detección y localización de objetos reflectantes tales como aeronaves, buques, naves espaciales, vehículos, personas y elementos meteorológicos del medioambiente. Opera radiando energía al espacio y detectando el eco de la señal reflejada desde un objeto o blanco [4]. La energía reflejada que retorna al radar no solo indica la presencia de un blanco, sino que comparando la señal reflejada con la señal que fue transmitida, se puede determinar su localización junto con otra información relacionada con el blanco. Los radares pueden desarrollar su tarea a cortas o largas distancias y bajo condiciones imposibles para sensores ópticos e infrarrojos. Pueden operar en la oscuridad, neblina, niebla, lluvia y nieve. Su habilidad para medir distancia con gran exactitud y en toda condición de tiempo es uno de sus mayores atributos.

La palabra "RADAR" en si es una sigla en inglés correspondiente a *"Radio Detection and Ranging"*. El principio básico de un radar es ilustrado en la Figura 2.7. Un transmisor genera una señal electromagnética (como un pulso muy corto de onda sinusoidal) que es radiado al espacio por una antena. Una porción de la energía transmitida es interceptada por el blanco y rerradiada en muchas direcciones. La rerradiación dirigida de vuelta hacia el radar es recolectada por su antena, que la entrega al receptor. Ahí es procesada para detectar la presencia del blanco y determinar su localización. Usualmente se utiliza una sola antena en una base de tiempo compartido para transmitir y recibir la forma de onda del radar, que es en sí una serie repetitiva de pulsos. El rango o distancia a un blanco se determina por medio de la medición del tiempo que le toma a la señal del radar para viajar al blanco y regresar de vuelta al mismo radar. Los ingenieros utilizan el término rango para referirse a distancia. La localización del blanco en ángulo se determina por la dirección en la que la antena del radar está apuntando cuando la señal de eco recibida es de máxima amplitud, para lo que la antena

se encuentra naturalmente georreferenciada. Si el blanco está en movimiento, habrá una variación en la frecuencia de la señal reflejada debido al efecto *doppler*. Esa variación en frecuencia es proporcional a la velocidad del blanco relativa al radar. La variación de frecuencia doppler es ampliamente utilizada en radares como la base para separar los blancos móviles deseados de los ecos fijos *(clutter)* no deseados, producto del reflejo de la señal en componentes del ambiente natural tal como el terreno, el mar o la lluvia. El radar también puede entregar información acerca de la naturaleza del blanco que está siendo observado.

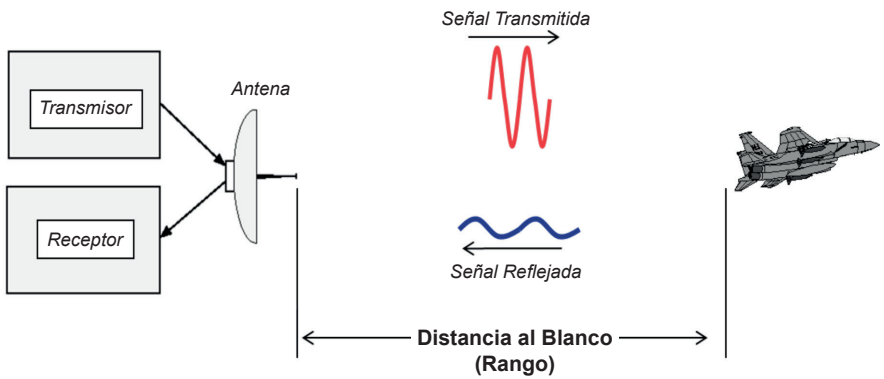

Figura 2.7: Principio básico de radar [4].

Rango, la distancia a un blanco. La señal de radar más común es una serie de pulsos de corta duración de forma rectangular modulando una portadora sinusoidal, también llamado tren de pulsos. El rango a un blanco se determina por el tiempo T_R que le toma a la señal del radar para viajar al blanco y volver. La energía electromagnética viaja a la velocidad de la luz en el espacio libre, que corresponde a c = 3 x 10^8 m/s. Por lo tanto el tiempo que le toma a una señal para viajar hacia el blanco localizado a un rango R y regresar devuelta al radar es 2R/c. Entonces, el rango a un blanco es

$$R = \frac{cT_R}{2}$$

Con el rango en kilómetros o en millas náuticas y T en microsegundos, la ecuación queda:

$$R(km) = 0{,}15T_R \qquad o \qquad R(nmi) = 0{,}081T_R$$

Cada microsegundo de tiempo en un viaje de ida y regreso corresponde a una distancia de 150 metros, 164 yardas, 492 pies, 0,081 millas náuticas o 0.093 millas estatutas. Toma 12,35 microsegundos a una señal de radar viajar una milla náutica y regresar.

Rango Máximo No ambiguo

Una vez que una señal es radiada al espacio por un radar, debe pasar suficiente tiempo para permitir que todas las señales eco (o reflejadas) retornen al radar antes de que el próximo pulso sea transmitido. Por lo tanto, la razón a la cual los pulsos pueden ser transmitidos está determinada por el máximo rango al que se espera que el radar detecte un blanco. Si el tiempo entre pulsos T_p es muy corto, el eco de una señal de un blanco a gran distancia puede llegar después de la transmisión del pulso siguiente y ser erróneamente asociado con ese segundo pulso y no con el pulso transmitido anteriormente. Esto puede generar una medida errónea o ambigua del rango. Los ecos que llegan después de la transmisión del pulso siguiente son llamados ecos de segunda vuelta. Este tipo de ecos parecen estar a rangos más cercanos que el real y su medición de rango puede confundir si no se sabe que son ecos de segunda vuelta. El rango superior al que los blancos aparecen como ecos de segunda vuelta es el rango no-ambiguo máximo *Run*, y está dado por

$$R_{un} = \frac{cT_p}{2} = \frac{c}{2f_p}$$

, donde T_p= período de repetición de pulsos = $1/f_p$, y f_p = frecuencia de repetición de pulsos (PRF), usualmente en Hertz o pulsos por segundos (pps).

Forma de Ondas de Radar

Un radar típico utiliza una forma de onda pulsada como el de la Figura 2.8. La potencia peak en este ejemplo es P_t = 1MW, ancho de pulso τ = 1 μs, período de repetición de pulsos T_p= 1ms = 1000 μs. La frecuencia de repetición de pulsos f_p es 1000 Hz, que proporciona un rango no ambiguo máximo de 150 km, o 81 nmi, La potencia pro-

medio (P_{av}) de una forma de onda de tren de pulsos repetitivo es igual a, $\frac{P_t \tau}{T_p} = P_t \tau f_p$ entonces la potencia promedio en este caso es $10^6 \times 10^{-6} / 10^{-3} = 1$ kw.

El ciclo de trabajo de una forma de onda de radar está definido como la razón del tiempo total en que el radar está irradiando dividido por el tiempo total que podría haber radiado, que está dado por $\tau/T_p = T f_p$, o su equivalente $\frac{P_{av}}{P_t}$. En este caso el ciclo de trabajo es 0,001.

La energía del pulso es igual a $P_t \tau$, que es 1 J (joule). Si el radar puede detectar una señal de 10^{-12} W, el eco estará 180 dB bajo el nivel de la señal que fue transmitida. Una forma de onda pulsada de corta duración es atractiva debido a que una fuerte señal transmitida no es irradiada cuando la señal débil de eco está siendo recibida.

Con un ancho de pulso τ de 1 μs, la forma de onda se extiende en el espacio sobre una distancia $C\tau$=300 m. Dos blancos iguales pueden ser reconocidos si son diferenciados en rango cuando ellos están separados una distancia igual a la mitad de ese valor, o $C\tau/2$. El factor medio es el resultado del viaje de ida y vuelta de la onda de radar. Por ejemplo, cuando τ=1 μs, dos blancos de igual tamaño pueden ser diferenciados en distancia si se encuentran separados por 150 m.

Los radares de largo alcance requieren un pulso muy largo para liberar energía suficiente y detectar pequeños blancos a larga distancia. Un pulso largo, sin embargo, tiene una resolución muy pobre en distancia. Se puede utilizar modulación en frecuencia o en fase para incrementar el ancho espectral de un pulso y así obtener una resolución similar a la de un pulso corto, esto es llamado compresión de pulso. Formas de onda del tipo onda continua (CW - *continuous wave*) también han sido utilizadas en radares. Como este tipo de radares deben recibirlas mientras están transmitiendo, los radares CW dependen de la variación de frecuencia *doppler* de la señal reflejada, causada por el movimiento de un blanco, para separar en el dominio de la frecuencia la débil señal reflejada de la gran señal transmitida y las reflexiones generadas por *clutter* (tierra, mar o atmósfera), así también como medir la velocidad radial del blanco. Un radar CW no mide distancia, sin embargo obtiene el rango por medio de la modulación de la portadora con modulación de frecuencia o fase.

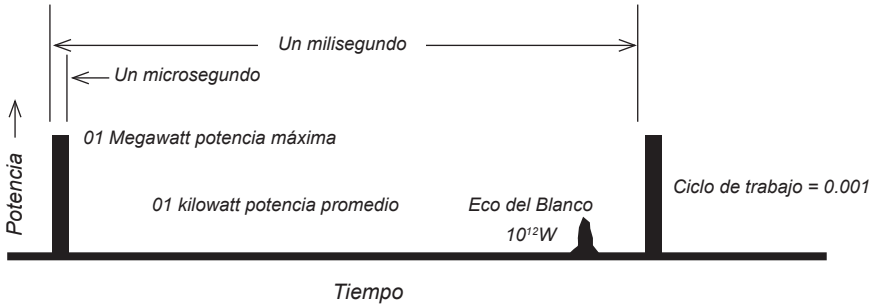

Figura 2.8: ejemplo de forma de onda pulsada. Valores típicos para un radar de vigilancia aérea de alcance medio. Los pulsos rectangulares representan las ondas sinusoidales moduladas en pulsos [4].

Los radares pulsados que extraen la variación de la frecuencia *doppler* son llamados "Moving Target Indicator"a (MTI) o "Radares Pulso Doppler", dependiendo de sus valores particulares de la frecuencia de repetición de pulsos (PRF) y ciclo de trabajo. Un radar MTI tiene un ciclo de trabajo y una PRF bajos. Un radar de pulso *doppler* por otra parte, tiene un ciclo de trabajo y una PRF altos. Casi todos los radares diseñados para detectar aeronaves usan la variación de frecuencia *doppler* para rechazar la gran cantidad de ecos no deseados de *clutter* estacionario.

La transmisión de los radares pulsados corresponde a pulsos de frecuencia fija separados por períodos de silencio durante los cuales los ecos de los pulsos son recibidos. Como se puede ver en la Figura 2.9, la modulación de pulsos se caracteriza por un ancho de pulso, un intervalo entre pulsos y la amplitud del pulso. El ancho de pulso (PW- *pulse width*) es la duración del pulso. El intervalo entre pulso es el tiempo entre el inicio de un pulso, hasta el inicio del siguiente pulso. El intervalo entre pulso en una señal usualmente es conocido como intervalo de repetición de pulsos (PRI) o la frecuencia de repetición de pulsos (PRF). El ancho de pulso y la razón de repetición son los mismos a la salida del transmisor, los mismos en el blanco o en el receptor mientras el radar y el blanco no se muevan (fijos), pero la amplitud del pulso varía considerablemente. La amplitud del pulso en una señal irradiada es la intensidad de esa señal. La medición obtenida en el instante en que el pulso deja la antena transmisora, entrega la potencia efectiva irradiada (ERP). Luego cuando el pulso

alcanza al blanco, la amplitud del pulso es la potencia instantánea aplicada al blanco y así cuando la señal reflejada llega al receptor del radar, esta es la intensidad de señal recibida.

El ciclo de trabajo de un radar es la razón del ancho de pulso al intervalo entre pulsos. Para un radar pulsado, su ciclo de trabajo puede ser desde 0,1 hasta 20%. Este ciclo de trabajo tan bajo significa que la potencia promedio de salida del radar es considerablemente más baja que su potencia máxima *(peak)*.

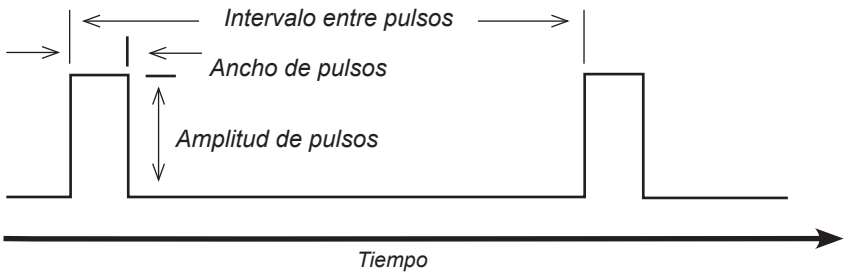

Figura 2.9: Características de una señal pulsada de radar. Fuente: elaboración propia.

La Ecuación de Radar [4]

La ecuación de radar relaciona el rango de un radar a las características del transmisor, receptor, antena, blanco y el medio en el cual se encuentran. Es muy útil no solo para determinar el rango máximo al que un radar en particular puede detectar un blanco, sino que sirve como medio para entender los factores que afectan el desempeño del radar. También es una herramienta importante para ayudar en el diseño de sistemas de radar.

Si la potencia del transmisor P_t es radiada por una antena isotrópica (antena que irradia uniformemente en todas direcciones), la densidad de potencia a una distancia R desde el radar será igual a la potencia irradiada dividida por el área de la superficie $4\pi R^2$ de una esfera imaginaria de radio R:

$$\text{Densidad de potencia al rango R desde una antena isotrópica (Watts)} = \frac{P_t}{4\pi R^2}$$

La densidad de potencia se mide en unidades de watts por metro cuadrado. Sin embargo, los radares emplean antenas directivas (con *beams* o haces angostos), para concentrar la potencia irradiada P_t en una dirección particular. La ganancia de una antena es una medida de la densidad de potencia irradiada incrementada en alguna dirección, comparada con la densidad de potencia que aparecería en aquella dirección desde una antena isotrópica. La ganancia máxima G de una antena puede definirse como:

G = (densidad de potencia máxima radiada por una antena direccional) / (densidad de potencia radiada por una antena isotrópica).

Entonces, la densidad de potencia en el blanco desde una antena direccional con una ganancia de transmisión G es:

$$\text{Densidad de potencia a un rango R desde una antena direccional} = \frac{P_t G}{4\pi R^2}$$

El blanco intercepta una porción de la energía incidente y la rerradia en varias direcciones. Solamente la densidad de potencia rerradiada en la dirección del radar (la señal ecorreflejada) es de interés. La sección cruzada de radar del blanco determina la densidad de potencia que retornará al radar, debido a una densidad de potencia incidental sobre el blanco. La sección cruzada de radar de un blanco se denota con las siglas RCS (*Radar Cross Section*, en inglés), con el símbolo σ y se define por la ecuación:

$$\text{Densidad de potencia rerradiada devuelta al radar} = \left(\frac{P_t G}{4\pi R^2}\right)\left(\frac{\sigma}{4\pi R^2}\right)$$

La RCS tiene unidades de área, pero erróneamente se asocia directamente con el tamaño físico del blanco. La RCS depende más de la forma, material y textura de la superficie del blanco que del tamaño, está incluida en la ecuación de radar para representar la magnitud de la señal reflejada hacia el radar por el blanco. Así se puede definir la RCS como:

$$\sigma(m^2) = \frac{\textit{potencia reflejada hacia el radar / unidad de ángulo sólido}}{\textit{densidad de potencia incidente} / 4\pi} = 4\pi R^2 \frac{|E_r|^2}{|E_t|^2}$$

, donde R es el rango al blanco, E_r es la intensidad del campo eléctrico de la señal reflejada hacia el radar y E_t es la intensidad del campo eléctrico incidente sobre el blanco. Se asume que el blanco se encuentra

lo suficientemente lejos del radar, de tal forma que la onda incidente puede ser considerada plana en vez de esférica. La RCS depende de la geometría, reflectividad y directividad del blanco, donde la geometría está determinada por el tamaño y forma del blanco según sea su aspecto visto desde el radar. La reflectividad es la razón de toda la potencia que refleja el blanco versus la potencia que lo ilumina, el resto de la potencia es absorbida o disipada. La directividad es la razón de la potencia reflejada hacia el radar versus la cantidad de potencia reflejada en todas direcciones. Bajo estos criterios la fórmula para la RCS es:

$$\sigma = \text{sección geométrica cruzada x Reflectividad x Directividad}$$

La RCS de una aeronave o un buque es una suma de vectores de la reflexión desde cada parte física de estos. Es muy irregular según su ángulo de aspecto y varía con la frecuencia de operación del radar. Puede ser medida en una cámara anecoidal que mide las reflexiones de las señales de radar sobre un blanco, partes de un blanco o un modelo a escala de un blanco. Existen algunos modelos asistidos por computadores, desarrollados para representar el blanco por medio de un número de superficies reflectoras que permiten calcular la RCS total a partir de la combinación ajustada de fases de las reflexiones de todas las superficies. Así se llega a la concepción de una ganancia efectiva en el camino de la transmisión de la señal de radar, que está en función de la RCS, que puede ser representada por la siguiente ecuación:

$$G\,(dB) = -39 + 20\log(F) + 10\log(\sigma)$$

, donde G es la razón de la señal que sale del blanco (reflejada) a la señal llegando al blanco en dB, F es la frecuencia de transmisión en MHz y σ es la RCS del blanco en m^2.

La siguiente Figura 2.10 a, muestra la RCS versus ángulo en el plano horizontal de un avión y la Figura 2.10 b, muestra la RCS típica de un buque desde un ángulo de elevación de 45° en función del plano horizontal. La unidad de medida es el dBsm, que son decibeles relativos a un metro cuadrado. Se debe notar que ambos diagramas presentan grandes variaciones en la magnitud de RCS dependiendo del ángulo desde dónde sean observadas, es decir que para aproximarse a un ra-

dar determinado deben considerar aquellos ángulos desde los cuales entregan una menor RCS hacia el radar adversario. También se debe tener presente que las RCS varían ampliamente con el tipo de avión o buque que se observe. La RCS de un avión es alta desde las partes frontal y trasera debido a los componentes del motor, sin embargo es mayor desde los lados debido a la mayor sección cruzada del fuselaje y los ángulos entre las alas y el fuselaje. Por otro lado, la RCS de un buque es típicamente simétrica con la forma de una estrella sobre el mismo y se caracteriza por un muy alto valor de RCS cada 90° desde la proa y menores para los tramos intermedios.

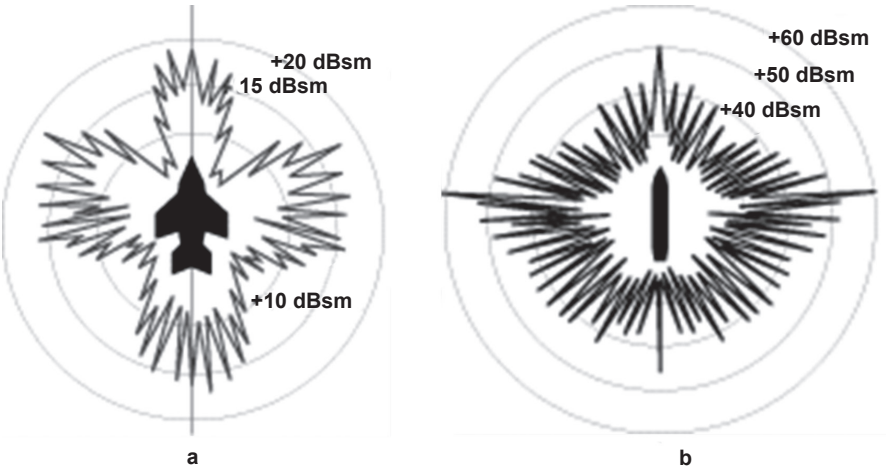

Figura 2.10: RCS de un avión (a) y de un buque (b), [5].

Actualmente se utilizan técnicas de diseño *"stealth"* que hacen uso de conocimiento avanzado en el diseño geométrico de la superficie y estructuras de las modernas aeronaves y buques de guerra, así como el empleo de materiales absorbentes o poco reflectante de las ondas de radar y pinturas absorbentes de energía electromagnética. Con esta tecnología no se logra hacer invisible al blanco, como muchos autores sostienen, sin embargo con la reducción de su RCS la energía reflejada hacia el radar es considerablemente menor, lo que conlleva a que el radar no reciba la energía reflejada suficiente desde el blanco como para procesarla en su receptor, negando de esta forma su detección a distancias que sin esa tecnología habría sido perfectamente detectado por el radar. Consecuentemente, ante blancos con tecnología *stealth* el efecto en los radares es que retrasan o reducen los

rangos de detección a distancias muy cercanas a su emplazamiento, lo que retrasa la posibilidad de dar la alerta y generar la reaccionar de los sistemas de armas.

En la siguiente figura se observan algunos valores típicos de RCS:

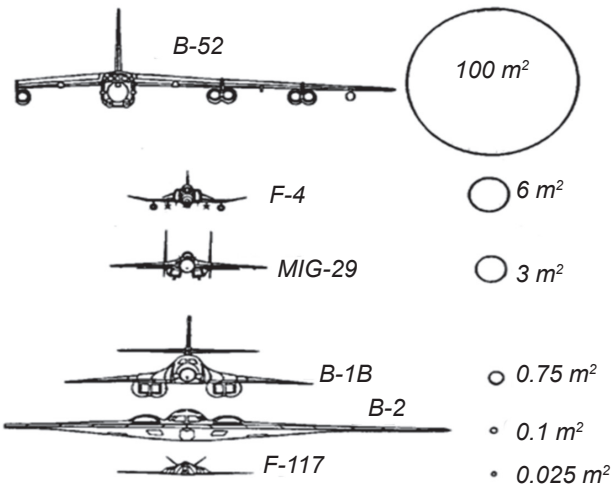

Figura 2.11: Sección cruzada de radar (RCS) de distintas aeronaves para una frecuencia determinada. Se debe notar la diferencia de RCS entre aeronaves de tecnología antigua versus moderna, pero de dimensiones similares, como es el caso del B-52 versus el B-1B, así también como el F-4 versus el F-117, [5].

Una vez reflejada la energía por la RCS del blanco, esta viaja de regreso al radar y su antena captura una porción de esa energía incidental. La potencia recibida por el radar está dada por el producto de la densidad de potencia incidental y el área efectiva A_e de la antena receptora. El área efectiva se relaciona con el área física A por la relación $A_e = \rho_a A$, donde ρ_a= eficiencia de la apertura de la antena. La potencia de la señal recibida P_r (watts) es dada por:

$$P_r(Watts) = \frac{P_t G}{4\pi R^2} \; x \; \frac{\sigma}{4\pi R^2} \; A_e = \frac{P_t G A_e \sigma}{(4\pi)^2 R^4}$$

El rango máximo de un radar R_{max} es la distancia más allá de la cual un blanco no puede ser detectado. Ocurre cuando la potencia de la señal recibida P_r iguala la señal mínima detectable por el receptor $S_{min} = P_r$, lo que genera:

$$R_{max} = \left(\frac{P_t G A_e \sigma}{(4\pi)^2 S_{min}} \right)^{1/4}$$

Esta es la forma fundamental de la ecuación de rango de radar, o simplemente la ecuación de radar. Los parámetros importantes de la antena son la ganancia de transmisión y el área efectiva de recepción. Para la potencia de transmisión P_t será considerada la potencia máxima o *peak*.

Si la misma antena es utilizada para transmitir y recibir, como usualmente sucede en un radar, la teoría de antenas entrega la relación entre la ganancia de transmisión G y el área efectiva de recepción A_e como:

$$G = \frac{4\pi A_e}{\lambda^2} = \frac{4\pi \rho_a A}{\lambda^2}$$

, donde λ = longitud de onda. (Longitud de onda $\lambda = \frac{c}{f}$, donde c = velocidad de propagación y f = frecuencia). Así la ecuación de radar se modifica según A_e y G, dando paso a otras dos formas de la ecuación de radar:

$$R_{max} = \left[\frac{P_t G^2 \lambda^2 \sigma}{(4\pi)^2 S_{min}} \right]^{1/4} \qquad R_{max} = \left[\frac{P_t A_e^2 \sigma}{4\pi \lambda^2 S_{min}} \right]^{1/4}$$

Estas tres formas de la ecuación de radar son básicamente las mismas con algunas diferencias en su interpretación. Estas versiones simplificadas de la ecuación de radar no describen adecuadamente el desempeño de un radar moderno, muchos factores no han sido explícitamente incluidos. Sin embargo, son mundialmente reconocidas y utilizadas para los cálculos involucrados en el diseño y estudio de los radares.

Aplicaciones del Radar

Los radares han sido utilizados para detectar blancos en tierra, en el mar, en el aire, en el espacio e incluso bajo tierra. Las aplicaciones del radar han cubierto las siguientes áreas:

- Militar: El radar es una parte importante de los sistemas de defensa aérea así como también de la operación de misiles y otros

sistemas de armas. En la defensa aérea desempeñan la función de vigilancia y control de fuego. La vigilancia incluye la detección, reconocimiento, seguimiento y designación de blancos a un sistema de armas. Los radares de control de fuego siguen a los blancos, dirigen las armas a interceptar el blanco y evalúan la efectividad del enfrentamiento. Un sistema de misiles puede emplear radares para guiado y activación de las armas. Los radares de imágenes de alta resolución, tales como los radares de apertura sintética son utilizados con propósitos de reconocimiento y para detectar blancos fijos y móviles en el campo de batalla. Por lo explicado en este punto es fácil inferir que los militares han demostrado ser quienes hacen el mayor uso del radar y el medio por el cual se han desarrollado las nuevas tecnologías en este campo.

- Sensores Remotos: Todos los radares son sensores remotos, sin embargo este término es utilizado para referirnos a sensores medioambientales. Cuatro ejemplos importantes son: la observación del clima, que constituye una de las fuentes de los reportes del tiempo que a diario observamos en televisión como así también la información primaria para las predicciones de meteorología, la observación planetaria, la investigación de cortas distancias bajo tierra y el levantamiento de mapas de hielo marino para las rutas de embarcaciones.

- Control de Tráfico Aéreo: Los radares han sido utilizados alrededor del mundo para el control seguro del tráfico aéreo en la cercanía de los aeropuertos y en las rutas desde un aeropuerto hacia otro, así como para el tráfico vehicular terrestre y el taxeo de los aviones en tierra. Aunque no es un radar, el IFF *(Identification Friend or Foe)* utiliza una tecnología confundida muchas veces con la de un radar por su similitud, pero es más a fin a un enlace de comunicación del tipo transponder automático que a un radar propiamente tal.

- Policía y Seguridad en Carreteras: El radar de control de velocidad, conocido por muchos, es utilizado por la policía para imponer los límites de velocidad.

- Seguridad en Aeronaves y Navegación: Los aviones de transporte mayor poseen radares para evitar condiciones climáticas adversas

que identifican zonas de precipitaciones y vientos peligrosos para permitir al piloto evitar esas condiciones de alto riesgo. Los aviones militares en vuelo bajo se apoyan en radares para navegar siguiendo el terreno y evitando colisionar con imperfecciones del mismo, en este caso el radar va formando un mapa del terreno y lo presenta como una imagen en la cabina para los pilotos. El radioaltímetro también es un radar utilizado para indicar la altura de un avión sobre el terreno.

- Seguridad en Barcos: Los radares se encuentran en embarcaciones para evitar colisiones y observar boyas de navegación, especialmente en condiciones de baja visibilidad. En la costa se utilizan radares similares para vigilancia de puertos y tráfico lacustre.

- Espacio: Grandes radares basados en la tierra son utilizados para la detección y seguimiento de satélites y otros cuerpos espaciales. El campo del radar en la astronomía ha utilizado sistemas basados en la tierra para ayudar a entender la naturaleza de los meteoritos, establecer una medición exacta de las mediciones astronómicas y la observación de la luna y los planetas cercanos, incluso antes de que se pudiera disponer de vehículos espaciales adecuados para explorarlos a corta distancia.

- Otros: El radar ha encontrado aplicaciones en la industria para la medición de velocidad y distancia. Ha sido utilizado para la exploración de gas y petróleo. Entomólogos y ornitólogos han aplicado el radar para estudiar el movimiento de insectos y aves, que no pueden ser fácilmente estudiados por otros medios.

El Radar Como Amenaza

Los radares son considerados como amenaza cuando corresponden a radares del tipo adquisición, de seguimiento *(tracking)* y radar tipo espoleta. La Tabla 2.3 muestra los parámetros de modulación típicos asociados a cada tipo de estos radares.

Los radares de adquisición ejecutan una búsqueda en grandes áreas para lograr la adquisición de blancos. Cuando los blancos son adquiridos estos son entregados a un radar de control de fuego. Los radares de adquisición son comúnmente llamados radares *"early warning"*, es decir de alarma temprana y se utilizan para la función de control de interceptación en tierra, porque estos también propor-

cionan localización del blanco para controladores que guían a los aviones de combate a interceptar estos blancos.

Los radares de control de fuego están asociados directamente con sistemas de armas. Un radar de control de fuego forma un archivo de seguimiento de un blanco (un archivo con información de velocidad y localización del blanco en seguimiento) de tal forma que un arma o misil pueda atacar al blanco en forma efectiva.

El propósito de un radar del tipo espoleta es activar la cabeza de guerra del arma a la distancia óptima del blanco. Para blancos de superficie esto es programado típicamente a una distancia estándar sobre la superficie. Para blancos aéreos, el radar determina cuando el blanco se encuentra dentro del alcance de la explosión de la cabeza de guerra, de tal manera que el blanco reciba el máximo número de proyectiles cuando la cabeza de guerra explote.

TIPO DE AMENAZA	RANGO OPERACIONAL	PARÁMETROS DE MODULACIÓN
Radar de adquisición	Muy largo alcance	Pulsos, largo ancho de pulso, baja PRF, comúnmente tiene compresión de pulsos
Radar de seguimiento *(trackeo)*	Corto alcance, alcance letal de armas asociadas	Pulso, pulso *doppler* u onda continua. Pulso corto, alta PRF. Radares de seguimiento modernos también pueden tener compresión de pulsos
Radares tipo espoleta	Muy corto alcance (unas pocas veces el radio letal de la cabeza de guerra)	Onda continua o pulsos de PRF muy alta

Tabla 2.3: Rango y modulación de los radares amenaza [3].

Ataque Electrónico Contra Radares *(Jamming)*

El propósito de todo *jamming* es interferir el uso efectivo que el adversario puede hacer del EEM. Como ya se expuso, el empleo del EEM involucra la transmisión de información desde un punto hacia otro. Esa información puede tomar la forma de comunicaciones de voz o

no (video o información en formato digital), señales de instrucciones para controlar remotamente algunos sistemas, data recolectada de dispositivos localizados remotamente o la localización y movimiento de las unidades amigas o adversarias (en el aire, mar o tierra).

Por muchos años el *jamming* ha sido llamado contramedida electrónica (CME), pero ahora su aceptación internacional es ataque electrónico. El ataque electrónico también incluye el empleo de altos niveles de potencia radiada o energía dirigida para dañar físicamente alguna capacidad adversaria. El *jamming* también es llamado *"soft kill"* debido a que puede hacer inefectiva o neutralizar alguna capacidad adversaria temporalmente, sin destruirla físicamente.

La técnica básica de *jamming* es introducir una señal en un receptor adversario junto con la señal esperada. El *jamming* llega a ser efectivo cuando la señal de interferencia en el receptor es lo suficientemente fuerte como para evitar que el adversario pueda extraer o recuperar la información que requiere de la señal que el espera, ya sea porque la información contenida en la señal que espera es cubierta por la potencia del *jamming* o debido a que ambas señales combinadas (la señal esperada y la señal de *jamming*) tienen características que impiden al procesador extraer apropiadamente la información deseada. La Tabla 2.4 define algunas formas en que se puede diferenciar los tipos de *jamming*. Más adelante se aborda una clasificación de los tipos de *jamming* y sus técnicas específicas.

TIPO DE JAMMING	PROPÓSITO
Jamming de comunicaciones	Interfiere con la habilidad del adversario para transmitir información sobre un enlace de comunicaciones.
Jamming de radar	Impide que el radar pueda adquirir blancos, evita el seguimiento de blancos o genera información falsa.
Jamming encubierto	Reduce la calidad de la señal deseada de tal forma que no puede ser apropiadamente procesada o tal que la información que transporta no puede ser recuperada.
Jamming de engaño	Induce al radar a procesar inadecuadamente su señal reflejada para indicar un rango o ángulo de arribo del blanco, incorrectos.
Señuelo	Parece más un blanco que el mismo blanco, causa que un arma guiada ataque el señuelo en vez del blanco.

Tabla 2.4: Tipos de *Jamming* [6].

El concepto más básico de aplicación del *jamming* es que este se aplica sobre el receptor y no sobre el transmisor. El análisis de una situación de *jamming* normalmente es confuso y es fácil cometer un error, así es que se debe recordar que para ser efectivo, el *jammer* debe introducir su señal en el receptor adversario, a través de la antena asociada. Por otro lado, esto depende de la intensidad de la señal que el *jammer* transmite en la dirección del receptor y la distancia y condiciones de propagación entre ambos [10].

Clasificación de *Jamming*

El *jamming* es usualmente clasificado de cuatro maneras: por el tipo de señal (radar versus comunicaciones), por la forma en que ataca al receptor (*jamming* de ruido versus de engaño), por la geometría del *jamming* (autoprotección versus *stand off*) y por la forma en que protege un sistema propio (señuelo versus el *jammer* original).

Jamming de Radar versus *Jamming* de Comunicaciones

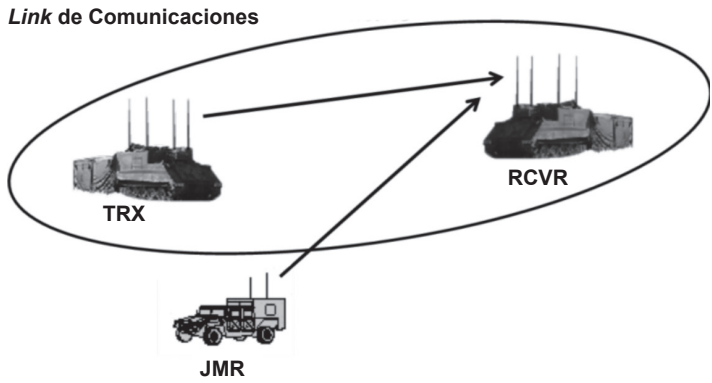

Figura 2.12: El *jamming* de comunicaciones interfiere con la habilidad del receptor para recuperar información de la señal esperada. Fuente: elaboración propia.

El *jamming* de comunicaciones es considerado normalmente el *jamming* de señales tácticas HF, VHF y UHF, que ruido modulado, pero también puede ser el *jamming* de enlaces de comunicaciones microondas punto a punto, o *data links* de mando o data pura, que transmiten de un punto a otro en forma remota. Según se muestra en la Figura 2.12, el enlace de comunicaciones adversario transporta una señal desde un transmisor (TRX) hacia un receptor (RCVR). El

jammer (JMR) también transmite hacia la antena del receptor, pero tiene suficiente potencia para superar las desventajas de ganancia de la antena (si la antena receptora tiene un haz angosto y se encuentra apuntando hacia el transmisor) y ser recibida y entregada al receptor o procesador con una potencia adecuada, para reducir la calidad de la información deseada a un nivel ilegible o al menos inutilizable.

Un radar clásico tiene un transmisor y un receptor, que utilizan una misma antena direccional. El receptor del radar está diseñado para recibir las señales reflejadas desde objetos que son iluminados por el transmisor y la antena del radar. El análisis de la señal reflejada permite al radar determinar la localización y velocidad de algunos ingenios terrestres, marinos o aéreos y seguirlos para propósitos amistosos (control de tráfico aéreo) o no amistosos (ataque por medio de armas guiadas, como misiles o cañones). El *jammer* de radar entrega una señal de engaño para evitar que el radar localice o siga un blanco, escenario que se puede apreciar en la Figura 2.13.

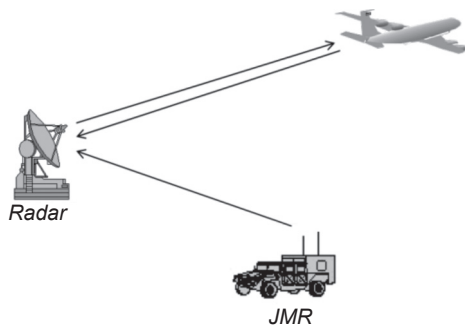

Figura 2.13: El *jamming* de radar, que puede ser del tipo ruido o de engaño, interfiere la habilidad del radar para recuperar la información del blanco desde su señal reflejada. Fuente: elaboración propia.

Jamming de Ruido versus *Jamming* de Engaño

El *jamming* de ruido involucra la transmisión de señales de alta potencia al receptor del adversario. El uso de la modulación de ruido hace más difícil para el enemigo saber que existe *jamming* en el lugar. Esto reduce la razón de señal a ruido (S/N) a un nivel tal que la señal esperada no puede ser recibida con la calidad adecuada. La Figura 2.14 muestra una pantalla de radar (*plan position indicator* - PPI) con una señal reflejada y *jamming* de ruido lo suficientemente fuerte como para esconder el eco. Idealmente el

jamming debe ser lo suficientemente fuerte para hacer imposible que un operador entrenado detecte la presencia de la señal, pero si es imposible o impracticable obtener esa gran cantidad de potencia del *jamming* en el receptor, será suficiente reducir la S/N al nivel que no se pueda realizar el seguimiento automático. Usualmente el procesamiento automático requiere una S/N significantemente mejor que la requerida por un operador entrenado para detectar y seguir una señal manualmente.

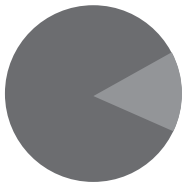

Figura 2.14: El *jamming* de ruido esconde la señal reflejada del radar al receptor/procesador. Fuente: elaboración propia.

El *jamming* de engaño hace que un radar entregue una conclusión errónea de la combinación de la señal esperada y la señal de *jamming*, según se muestra en la Figura 2.15. El *jammer* genera la radiación deliberada, rerradiación, alteración, absorción o reflexión de la EEM con la intención de confundir, distraer o seducir los sistemas electrónicos adversarios, por medio de la generación de blancos falsos. Normalmente, el *jamming* seduce al radar respecto del rango, ángulo y/o velocidad del blanco. Con el *jamming* de engaño, el radar recibe una señal reflejada aparentemente válida y erróneamente la considera un blanco válido.

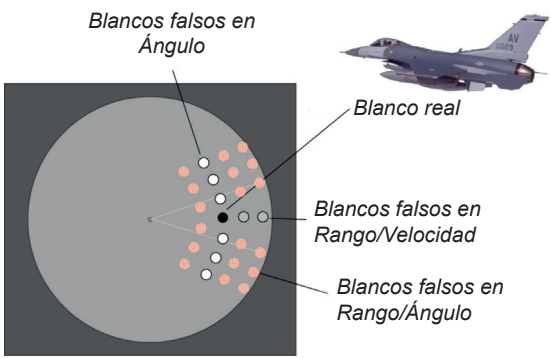

Figura 2.15: En la representación de una pantalla de radar se aprecia los resultados de las técnicas de engaño en ángulo, rango y velocidad. Fuente: elaboración propia.

Jamming de Autoprotección versus *Jamming Stand-Off*

El *jamming* de autoprotección y *stand-off* son ilustrados en la figura 2.16 y 2.17, respectivamente. Ambos son normalmente categorizados como *jamming* de radar, pero estas técnicas son aplicadas contra cualquier sistema adversario para proteger las capacidades propias de combate. El *jamming* de autoprotección se origina en un jammer transportado en la plataforma que está siendo detectada o seguida por el adversario. El *jamming stand-off* involucra un *jammer* en una plataforma que transmite señales de *jamming* para proteger otra plataforma. Normalmente, la plataforma protegida se encuentra en el rango letal de los sistemas de armas adversario y el *jammer stand-off* se encuentra fuera de ese rango.

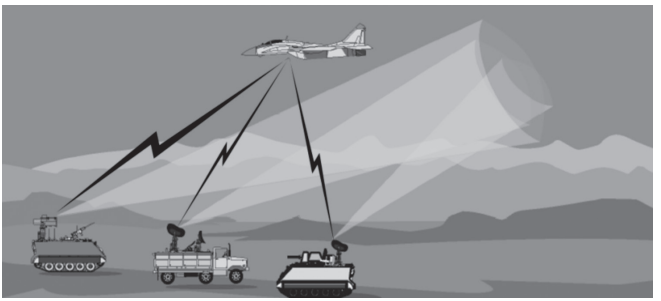

Figura 2.16: El *jamming* de autoprotección se origina en equipos *jammer* a bordo de la plataforma que está siendo seguida por uno o más radares, según se observa en esta figura. Como resultado los radares adversarios pierden el seguimiento del blanco [5].

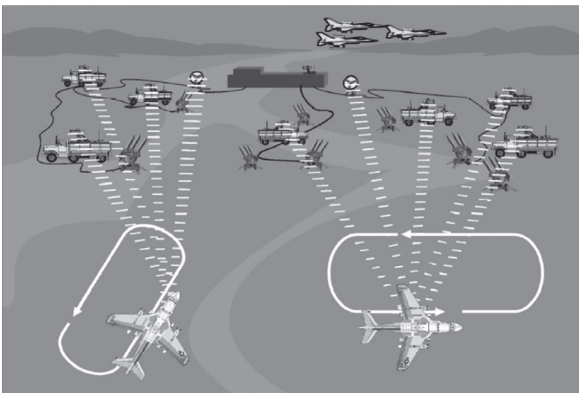

Figura 2.17: El *jamming stand-off* permite que un *jammer* de alta potencia a bordo de otra plataforma fuera del alcance de las armas adversarias, proteja las plataformas que están siendo seguidas por los radares adversarios y que normalmente se encuentran dentro del alcance del fuego adversario [5].

Señuelos (Decoys)

Un tipo especial de *jammers* son los señuelos, diseñados para asemejarse a una plataforma protegida ante un radar adversario, más que la plataforma original en sí misma. La diferencia entre los señuelos y otro tipo de *jammer* es que los señuelos no interfieren con la operación del radar que lo está siguiendo, más bien buscan atraer la atención de esos radares originando su adquisición y seguimiento e idealmente iniciar el fuego de los sistemas de armas en contra de ellos.

Razón *Jamming*-Señal (J/S)

La efectividad de un *jammer* es calculable solo en el contexto del receptor del adversario que está siendo afectado. La forma más común de describir la efectividad es en términos de la potencia efectiva del *jammer* (que es la potencia de la señal del *jammer* que alcanza los componentes internos del receptor), versus la potencia de la señal que el receptor realmente quiere recibir. Esto se llama razón de *jamming* a señal, o la razón de J a S, o simplemente J/S.

Existen muchos casos especiales en que la aplicación de la razón J/S debe ser modificada para mayor exactitud, de las cuales algunas serán cubiertas en este ensayo, pero todas están basadas en los principios que serán explicados en adelante. Las ecuaciones en forma de decibel (dB) utilizadas en esta discusión incluyen factores numéricos que representan de manera conveniente algunas leyes físicas constantes, permitir el ingreso de parámetros y obtener resultados directamente en las unidades más útiles. En este estudio las distancias están en km, todas las frecuencias están en MHz y la sección cruzada de radar (RCS) está siempre en m^2.

Potencia de la Señal Recibida (S)

Primero se debe considerar la señal como parte de la razón J/S. En el caso de una señal transmitida en una dirección desde un transmisor hacia un receptor, como se ve en la Figura 2.18, la señal llega al ingreso del receptor con un nivel de potencia definido por la ecuación:

$$S(dBm) = P_t + G_t - 32 - 20\log(F) - 20\log(D_s) + G_R$$

Donde P_t = potencia transmitida (en dBm); G_t = ganancia de la antena transmisora (en dB); F = frecuencia de transmisión (en MHz); D_S = distancia desde el transmisor al receptor (en km) y G_R = ganancia de la antena receptora (en dB).

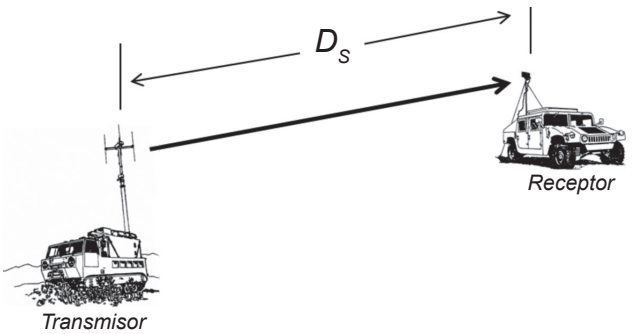

Figura 2.18: La señal deseada llega al ingreso del receptor con una intensidad determinada por la potencia del transmisor, ambas ganancias de las antenas y una pérdida de enlace determinada por la frecuencia de operación y la distancia del enlace. Fuente: elaboración propia.

Para el caso de una señal de radar, según se puede observar en la Figura 2.19, el transmisor y receptor son típicamente colocalizados y comparten la misma antena, de esta forma la señal llega al receptor con un nivel de potencia definido por la siguiente ecuación:

$$S = P_T + 2G_{T/R} - 103 - 20\log(F) - 40\log(D_T) + 10\log(\sigma)$$

, donde P_T = potencia del transmisor (en dBm); $G_{T/R}$= ganancia de la antena en transmisión/recepción (en dB); F = frecuencia de transmisión (en MHz); D_T = distancia desde el radar al blanco (en km) y σ = sección cruzada de radar del blanco (en m^2).

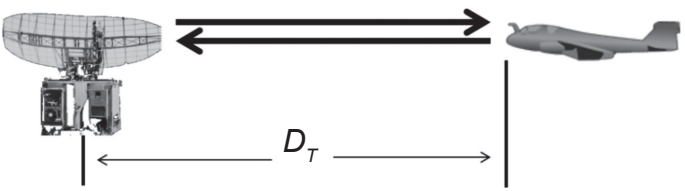

Figura 2.19: Una señal radar llega al receptor con una intensidad de señal determinada por el doble de su ganancia de antena, la distancia de ida y vuelta al blanco, la frecuencia de la señal y la sección cruzada de radar del blanco. Fuente: elaboración propia.

Potencia de *Jamming* Recibida (J)

Las señales de *jamming*, por su naturaleza, son transmisiones que tienen un solo sentido (un solo viaje de la señal, según se ve en la Figura 2.20). En general, el desempeño de la señal de *jamming* es el mismo ya sea ante un receptor de comunicaciones o un receptor de radar. Su aceptación por parte del receptor difiere de la señal esperada en dos formas. Primero, a no ser que el receptor tenga una antena omnidireccional, la ganancia de la antena varía en función del acimut o elevación con que la antena recibe las señales. Así, el *jamming* y la señal esperada experimentan distintas ganancias de recepción (ver Figura 2.21), a no ser que ambas lleguen desde la misma dirección. Segundo, las señales de *jamming* a menudo deben ser mucho más anchas en frecuencia que la señal a interferir, porque la frecuencia exacta de la señal deseada no puede ser fácilmente medida o estimada.

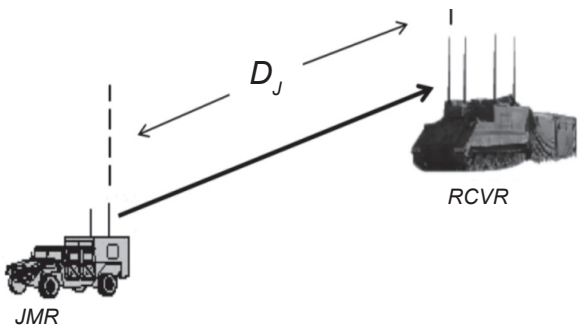

Figura 2.20: La señal de *jamming* llega al ingreso del receptor con su intensidad determinada por la potencia del transmisor, ganancia de la antena del *jammer*, pérdidas del enlace relacionadas a su frecuencia, la distancia del enlace y la ganancia de la antena receptora en la dirección del *jammer*.
Fuente: elaboración propia.

Al calcular la J/S es importante considerar solo la parte de la potencia de la señal de *jamming* que cae dentro del ancho de banda en que opera el receptor. Teniendo presente estas consideraciones, la potencia del *jamming* que llega al ingreso del receptor es definida por la ecuación (en dB):

$$J(dB) = P_J + G_J - 32 - 20\log(F) - 20\log(D_J) + G_{RJ}$$

, donde P_J = potencia de transmisión del *jammer* (en dB) dentro del ancho de banda del receptor; G_J = ganancia de antena del *jammer* (en dB); F= frecuencia de transmisión (en MHz); D_J = distancia entre el *jammer* y el receptor (en km) y G_{RJ} = ganancia de la antena receptora en la dirección del *jammer* (en dB).

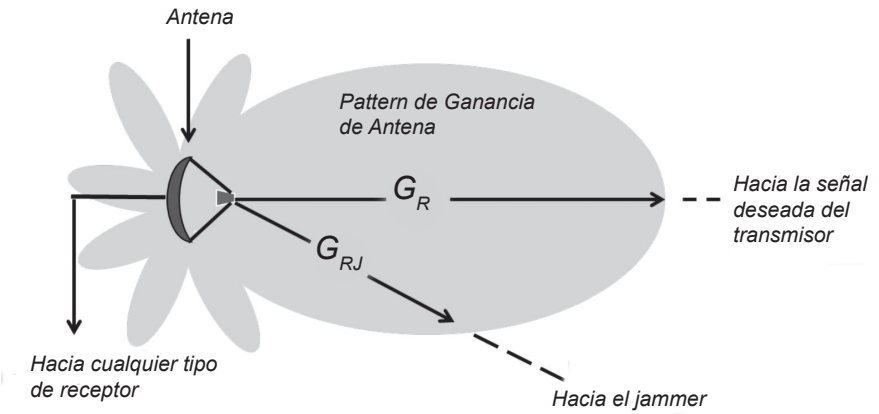

Figura 2.21: Si la antena receptora no es omnidireccional, su ganancia hacia la señal de *jamming* será diferente (normalmente menor) que su ganancia hacia la señal deseada. Fuente: elaboración propia.

Según se puede observar en la Figura 2.22, J/S es la razón de la intensidad de la señal del *jamming* (dentro del ancho de banda del receptor) respecto a la intensidad de la señal esperada. Se asume por supuesto, que el ancho de banda del receptor esta idealmente dimensionado y sintonizado a la señal esperada. Como el J y la S son expresadas en dB, su razón de potencia es simplemente la diferencia entre sus valores en dB. Para el caso de la transmisión de la señal en un solo sentido (aplicable principalmente para consideraciones de *jamming* de comunicaciones), la razón J/S en dB es:

$$J/S(dB) = J - S =$$

$$= P_J + G_J - 32 - 20\log(F) - 20\log(D_J) + G_{RJ} - [P_t + G_t - 32 - 20\log(F) - 20\log(D_s) + G_R] =$$

$$= P_J - P_T + G_J - G_T - 20\log(D_J) + 20\log(D_s) + G_{RJ} - G_R$$

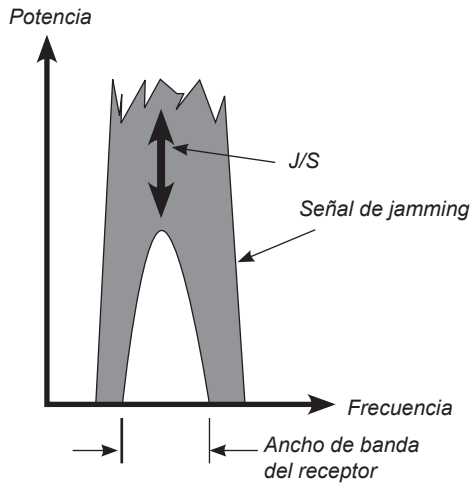

Figura 2.22: La razón *jamming* a señal es simplemente la razón de la potencia de ambas señales, recibidas dentro del ancho de banda del receptor.
Fuente: elaboración propia.

Burn-throug

El *burn-through* es un concepto muy importante en GE, ya que tiene que ver con las circunstancias operacionales bajo las cuales el *jamming* mantiene su efectividad contra un receptor víctima. El *burn-through* ocurre cuando la razón J/S se reduce al punto donde el receptor que está siendo atacado (jammeado) puede hacer su trabajo adecuadamente a pesar de estar sometido a la acción de *jamming*.

El Rango *Burn-through*

El rango *burn-through* se define en términos del *jamming* de radar, pero puede ser aplicado al *jamming* de comunicaciones también. En *jamming* de radar, el rango *burn-through* es la distancia al blanco a la cual el radar tiene una calidad de señal adecuada para continuar con el seguimiento del blanco. El rango donde el eco de la señal reflejada es igual a la señal del *jammer* corresponde al punto donde la razón J/S = 1 y debido a que la señal del radar debe viajar al blanco y luego volver, el *jammer* tiene una ventaja solo a mayores distancias. En la medida que el rango disminuye, el *jammer* pierde su efectividad y el radar puede adquirir el blanco. Solo dentro de la distancia *burn-through* el eco del blanco se verá con mayor intensidad que el *jamming* en la pantalla del radar. Esto obedece a una combinación de

la ecuación de densidad de potencia de la señal recibida (intensidad de señal) y la ecuación de potencia de *jamming* de ruido recibida. La Figura 2.23 muestra esta condición para *jamming* de autoprotección.

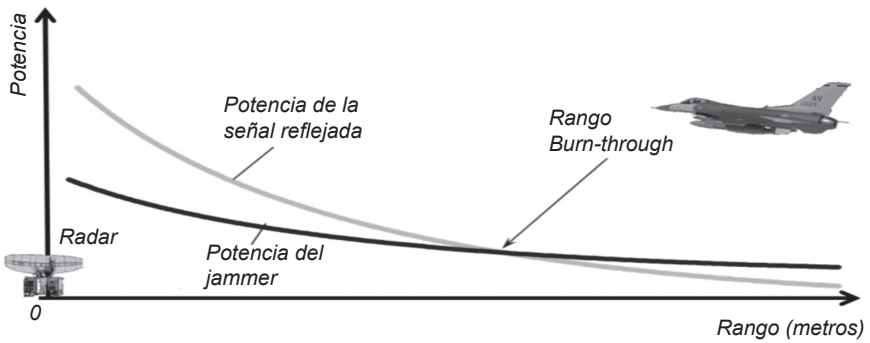

Figura 2.23: El rango *burn-through* es el rango desde el radar al blanco en el que el *jammer* no puede evitar que el radar cumpla su trabajo (detectar y seguir). Fuente: elaboración propia.

En *jamming* de comunicaciones, el concepto de rango *burn-through* no es tan gráfico, pero algunas veces útil. Para este caso el rango *burn-through* significa el rango efectivo del enlace de comunicaciones en la presencia de una aplicación de *jamming* específica, según se puede observar en la Figura 2.24. Es la distancia desde el transmisor al receptor, a la que el receptor tiene una adecuada razón de señal a ruido, para demodular y recuperar la información requerida desde la señal esperada.

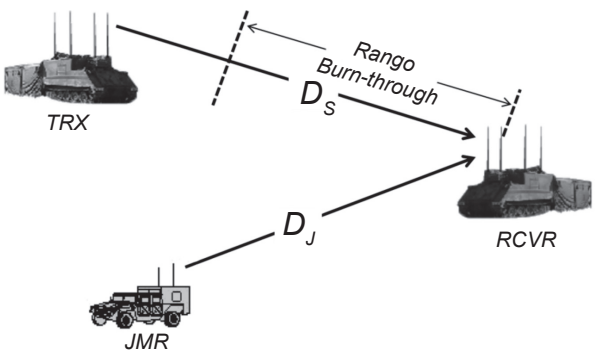

Figura 2.24: El rango *burn-through* de comunicaciones ocurre cuando el rango desde el transmisor al receptor es reducido a una distancia determinada, en la cual la señal puede ser recibida con una calidad aceptable. Fuente: elaboración propia.

Razón J/S Requerida

La razón J/S requerida para un *jamming* efectivo puede variar desde 0 a 40 dB o más, dependiendo del tipo de *jamming* empleado y de la naturaleza de la modulación de la señal esperada. Debido a que 10 dB de J/S es un buen valor aproximado que se aplica en muchas situaciones, se entenderá como un valor adecuado en este ensayo [6].

La fórmula para rango *burn-through* para cada tipo de *jamming* es solo la ecuación apropiada de J/S presentada con todos los términos definidos anteriormente, pero reordenada para aislar el parámetro correspondiente al rango. La fórmula J/S para *jamming* de radar del tipo *stand-off* es:

$$J/S = 71 + P_J - P_T + G_J - 2G_{T/R} + G_{RJ} - 20\log(D_J) + 40\log(D_S) - 10\log(\sigma)$$

, que puede ser reordenada como se indica a continuación:

$$40\log(D_S) = -71 - P_J + P_T - G_J + 2G_{T/R} - G_{RJ} + 20\log(D_J) + 10\log(\sigma) + J/S$$

La expresión $40log(D_S)$ puede ser calculada con los valores de los distintos parámetros de la señal y el *jamming*. Como este es el caso de un radar, se puede cambiar D_S por D_r (la distancia al blanco). D_r es un número en dB, que debe ser transformado a unidades de distancia (km). El rango *burn-through* es:

$$D_T(km) = 10^{\left(\frac{40\log(D_T)}{40}\right)}$$

Para el caso de *jamming* de radar del tipo autoprotección, la fórmula es:

$$J/S = 71 + P_J - P_T + G_J - G_{T/R} + 20\log(D_T) - 10\log(\sigma)$$

, que puede ser reordenada como se indica a continuación:

$$20\log(D_T) = -71 - P_J + P_T - G_J + G_{T/R} + 10\log(\sigma) + J/S$$

$$D_T(km) = 10^{\left(\frac{20\log(D_T)}{20}\right)}$$

La fórmula para la razón J/S en *jamming* de comunicaciones es:

$$J/S = P_J - P_T + G_j - G_T - 20\log(D_J) + 20\log(D_S) + G_{RJ} - G_R$$

, que puede ser reordenada como se indica a continuación:

$$20\log(D_S) = -P_J + P_T - G_J + G_T + 20\log(D_J) - G_{RJ} + G_R + J/S$$

, por lo tanto:

$$D_S(km) = 10^{\left(\frac{20\log(D_T)}{20}\right)}$$

El *jammer* que utiliza modulación de ruido, simplemente reduce en la medida de lo posible, la razón señal a ruido (S/N) en el receptor víctima. El *jamming* de engaño causa que un radar derive conclusiones falsas acerca de la localización o velocidad del blanco que pretende seguir.

Todo tipo de receptor debe tener una adecuada razón señal a ruido (S/N), con el objetivo de procesar adecuadamente las señales para las cuales está diseñado para recibir. La S/N es la razón de potencia de la señal deseada a la potencia del ruido en el ancho de banda del receptor. En un ambiente no hostil, la potencia del ruido es el ruido térmico del sistema receptor. La potencia recibida de la señal deseada está en función de la potencia de transmisión, la distancia de la transmisión, la frecuencia de operación y (solo para radares) la RCS del blanco. El *jamming* de ruido inyecta ruido adicional en el receptor, que tiene el mismo efecto que incrementar la distancia de transmisión o disminuir la RCS del blanco del radar.

Cuando el ruido del *jamming* es significativamente más alto que el ruido termal del receptor, se habla de la razón J/S en vez de S/N, pero el efecto en la recepción y procesamiento de la señal es el mismo. Si el *jamming* de ruido se incrementa gradualmente, el operador o el circuito de procesamiento automático que sigue al receptor, puede que nunca se dé cuenta de la presencia del *jamming*, solo que la S/N se está tornando extremadamente baja.

La S/N requerida depende de la naturaleza de la señal recibida y el modo en que es procesada para extraer su información. Para comu-

nicaciones de voz la comunicación efectiva cesa cuando la S/N se disminuye al punto en que ninguna información puede ser recibida. Para señales digitales, una S/N inadecuada origina bits erróneos y la comunicación cesa cuando la taza de bit erróneo (BER) es muy alta.

Para señales de radar, un operador entrenado puede seguir manualmente un blanco a una S/N mucho más baja que la requerida para un circuito de seguimiento automático, que maneja blancos múltiples. Por esto, el objetivo de un *jamming* de radar es derrotar la habilidad del radar para efectuar un seguimiento automático, haciendo que el radar llegue a saturarse con mucho menos blancos, como se puede apreciar en la Figura 2.25.

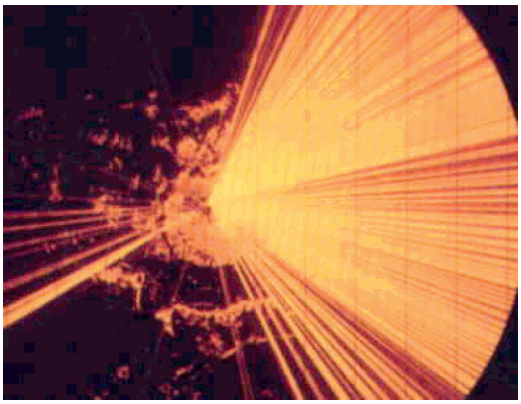

Figura 2.25: Pantalla de radar saturada producto de la acción de un *jamming* de ruido, con J/S considerablemente alta (S/N muy baja). [9].

Más Información acerca de Señuelos

Un señuelo es un dispositivo que está diseñado para que un radar adversario lo detecte, siga y considere más similar a un blanco verdadero que el mismo blanco. Los señuelos cumplen tres misiones primarias: saturan el sistema integrado de defensa aérea del adversario, obligan al adversario a exponer sus fuerzas prematuramente y evitan el seguimiento de radares adversarios.

Señuelos de Saturación

Un señuelo de saturación es generalmente un vehículo desechable que es diseñado para emular un blanco que penetra en el rango de

detección efectivo de los sensores adversarios. Su misión es engañar y saturar los sistemas de defensa adversarios. Empleando múltiples señuelos de saturación se puede forzar a los sistemas de defensa adversarios a dedicar recursos críticos para enfrentar estos objetivos falsos. Esto agota las capacidades adversarias disponibles para enfrentar a las fuerzas propias. Además, los señuelos de saturación pueden ser lanzados desde el suelo o el aire, utilizándolos para estimular los sistemas de arma adversarios, y de esta forma reunir data de inteligencia, o para iniciar ataques de supresión de sistemas de defensa adversaria. Las tres características principales de los señuelos de saturación son su firma electrónica (RCS en el caso de radares), su programa de vuelo y su tipo de misión.

Los señuelos de saturación deben presentar una firma electrónica, o eco de radar, que no se pueda diferenciar del blanco que pretenden proteger. Los señuelos pueden hacer esto por medidas pasivas o activas, o utilizar una combinación de ambas. Un señuelo pasivo es en esencia un reflector de ondas de radar. El tamaño, la forma, y los materiales utilizados en el señuelo son optimizados para asegurar que la cantidad apropiada de energía de radar sea reflejada a los radares adversarios. Los señuelos activos emplean sistemas de repetición de señales que reciben la señal del radar adversario, la amplifican y retransmiten un eco del tamaño apropiado para confundir al radar adversario. Reflejar o retransmitir el tamaño apropiado del eco de radar es crítico para ambos señuelos, pasivos y activos. Un eco que es demasiado grande o demasiado pequeño permitirá al operador de radar adversario diferenciar entre señuelos y blanco, causando que los señuelos sean ignorados.

Para continuar engañando los sistemas de armas adversarios, un señuelo debe no solo proporcionar la reflexión de radar apropiada en tamaño, sino que debe poseer características de vuelo semejantes al avión que protege. Esto aumentará la probabilidad de que el señuelo sea efectivamente seguido por los sistemas adversarios por un espacio de tiempo sostenido. Los señuelos modernos pueden contar con cohetes, motores miniaturizados o simplemente deslizarse por distancias muy largas gracias a la altitud y velocidad que tenga la aeronave que los libere o la artillería que los lance. Adicionalmente, sus trayectorias de vuelo pueden ser programadas a bordo en un sistema tipo piloto automático, permitiendo al señuelo volar una ruta

independiente, aumentando así su apariencia de avión de ataque que justifica su seguimiento por parte de los sistemas adversarios.

Los señuelos de saturación realizan dos de las tres misiones. Lanzados en números significativos, pueden saturar o pueden sobrecargar un sistema de defensa adversario. Mientras tanto, su imagen electrónica real y trayectorias de vuelo preprogramadas inducen al adversario a encender radares y mostrar el despliegue de sus fuerzas.

Señuelos de saturación lanzados en coordinación con un grupo de ataque, forzarán al enemigo a gastar tiempo en procesar blancos sin sentido y asignar sistemas de armas críticos contra los señuelos. Por esa razón, los señuelos trabajan primeramente contra la red de alarma temprana del adversario, presentando numerosos blancos para ser procesados, clasificados y seguidos. De esta manera, los recursos comprometidos en buscar y seguir señuelos no estarán disponibles para buscar y seguir los blancos verdaderos. Adicionalmente, si un adversario sabe que se encuentra en presencia de señuelos, podría dudar en comprometer recursos (armas) contra los blancos por temor a que solo sean señuelos.

El tiempo de radiación o el control de emisión es un factor crítico para los radares de adquisición y seguimiento de blancos. Para ser efectivos y sobrevivir en el campo de batalla, los radares amenaza de superficie irradian lo menos posible; demasiado tiempo irradiando le permite a los sistemas de inteligencia electrónica encontrar su ubicación e instruir a las fuerzas propias para evitarlos o generar un ataque contra ellos. Por lo tanto, cuando un señuelo puede conseguir que un radar emita, el radar queda expuesto y puede ser evitado o atacado. Conseguir que los radares del adversario emitan, generalmente constituye una acción precursora a cualquier misión de supresión contra ese sistema (destrucción), por medio de misiles antirradiación lanzados desde fuera del alcance letal de las armas del adversario.

Los señuelos de saturación pueden ser o pasivos o activos, pero deben proporcionar una RCS aproximadamente igual a la del blanco. Ellos también deben proporcionar otras características perceptibles para el radar que deben ser lo suficientemente semejantes a las del blanco para “engañar” al radar. Un ejemplo de un señuelo pasivo de

distracción es mostrado en la Figura 2.26. Aquí, el *chaff* provee una RCS cercana a la del buque que está protegiendo. El lanzamiento del chaff debe obedecer a una secuencia tal que un sistema de armas controlado por radar deberá procesar cada nube de chaff como si fuera el blanco.

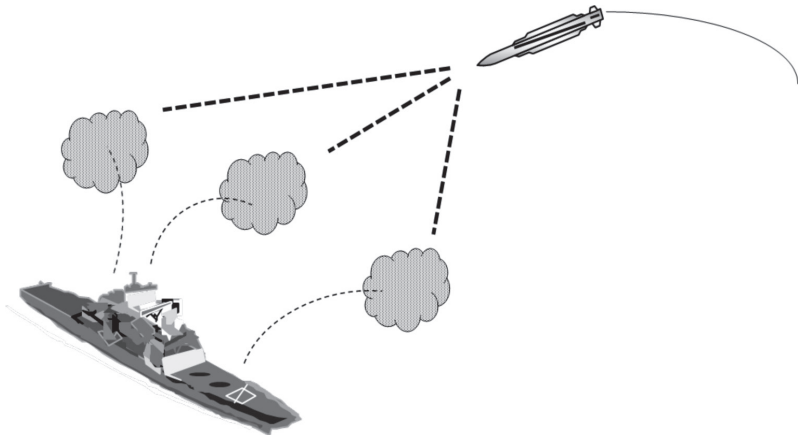

Figura 2.26: Un buque dentro del despliegue de nubes de *chaff* a babor que entregan una RCS similar a la del buque, llevará al radar a bordo de un misil a evaluar muchos blancos para encontrar el verdadero. Esta maniobra se hace más difícil aún para el misil, ya que el buque maniobrará y las nubes de *chaff* se moverán con el viento. Fuente: elaboración propia.

Señuelos de Seducción

En la misión de seducir, el señuelo debe atraer la atención de un radar que ha establecido el seguimiento de un blanco, causando que el radar cambie su seguimiento hacia el señuelo, entonces el señuelo se aleja del objetivo. Los radares de seguimiento solo trabajan con segmentos angostos de acimut (y a veces de elevación), rango y frecuencia de la señal reflejada. Para esto extraen los parámetros de la señal recibida para clasificarlos en compuertas de ángulo, distancia y frecuencia que componen el mecanismo de seguimiento de blancos. Si el señuelo puede mover y/o modificar cualquiera o todas esas compuertas, lo suficientemente lejos del blanco verdadero, el seguimiento sobre el blanco se quebrará. Es por esto que se llaman señuelos de seducción. Su función es muy similar a la de un *jammer* de engaño, sin embargo, el señuelo es más poderoso porque mantiene la atención del

radar que continúa siguiéndolo. El *jammer* de engaño por otro lado, extrae por ejemplo la compuerta de distancia del radar a una ubicación que no contiene un blanco, permitiendo al radar tratar de readquirir el blanco. Otra ventaja del señuelo es por supuesto, que sus señales son transmitidas desde una ubicación lejana al blanco real.

Como se puede ver en la Figura 2.27, un señuelo de seducción debe encenderse dentro de la celda de resolución del radar cuando este ya tiene adquirido al blanco que se pretende proteger, entonces para ser efectivo el señuelo debe transmitir hacia el radar una señal con suficiente potencia como para simular una RCS significantemente mayor a la del blanco a defender. Se debe tener presente que la RCS del blanco está en función del acimut y elevación desde donde es visto y paralelamente el hecho de maniobrar para reducir su RCS expuesta al radar puede ser una parte integral de su estrategia de defensa. Como se puede ver en la Figura 2.27 a), el señuelo captura el mecanismo de seguimiento del radar, por lo que la celda de resolución se desplaza para centrarse sobre el señuelo y comienza a separarse del blanco, según se puede ver en la Figura 2.27 b y c. En este caso el señuelo va quedando detrás del blanco, pero si el señuelo tuviera autopropulsión, perfectamente podría haberse alejado del blanco en cualquier dirección. Si el señuelo tiene éxito, desplazará la celda de resolución del radar lo suficientemente lejos y dejará al blanco fuera de esta. Es importante lograr que el radar no pueda distinguir el señuelo del blanco, si el radar logra percibir algún parámetro de la señal reflejada que el señuelo no pueda reproducir, el radar ignorará el señuelo y continuará con el seguimiento del blanco. Algunos ejemplos de este tipo de parámetros son los efectos relacionados con el tamaño y la forma del blanco, como así también la modulación que los motores jet de los aviones de combate generan sobre la señal reflejada. En otras palabras, existe un tipo de juego de torero al utilizar señuelos por parte del blanco, es decir para poder seducir al radar adversario primero este debe adquirir el blanco y una vez en función de seguimiento, este último puede utilizar un señuelo que se active dentro de la celda de resolución para llevar el seguimiento del radar contra el señuelo, así el radar perderá definitivamente al blanco. Así, la capa roja del torero pasa a ser el señuelo, el que se presenta dentro del campo visual del toro, que vendría siendo el radar.

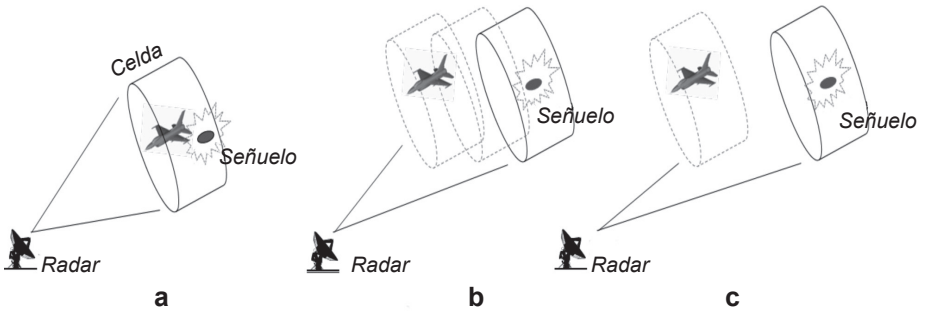

Figura 2.27: El radar inicialmente centra su celda de resolución en el blanco. Luego, el señuelo de seducción se activa dentro de la celda de resolución, presentando una RCS significativamente mayor a la del blanco. Esa RCS del señuelo hace que la celda de resolución del radar siga al señuelo a medida que se aleja del blanco. Fuente: elaboración propia.

La Figura 2.28 es una representación simplificada de la RCS, observada por el radar durante la secuencia de operación del señuelo. Esta figura ignora el efecto geométrico de los cambios de orientación del blanco relativos al radar, así como también la variación del rango entre el radar y el blanco.

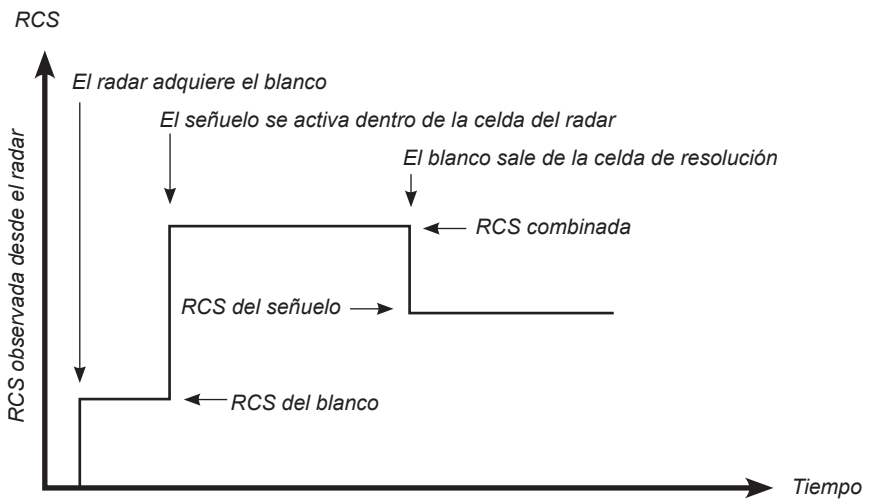

Figura 2.28: La mayor RCS del señuelo de seducción, captura las compuertas de seguimiento del radar. Fuente: elaboración propia.

La Figura 2.29 muestra imágenes de una pantalla de radar de control de fuego, que presenta la amplitud de la señal recibida en el eje verti-

cal y la distancia al blanco en el eje horizontal. La imagen de la letra a, presenta la detección de un blanco (avión de combate) con un pulso limpio y nítido (señal reflejada por el blanco). La imagen de la letra b, muestra el ensanchamiento del pulso producto del aumento de la RCS debido al lanzamiento de un señuelo (nube de *chaff*). La imagen de la letra c y d, muestran el seguimiento que hace el radar sobre el pulso de mayor RCS que corresponde a la nube de *chaff*, mientras el pulso reflejado por el blanco se encuentra fuera de la celda de resolución y se desplaza hacia el radar, es decir el avión se aproxima para efectuar su ataque, libre de que algún sistema de armas adversario pueda recibir información respecto de el por parte del radar atacado.

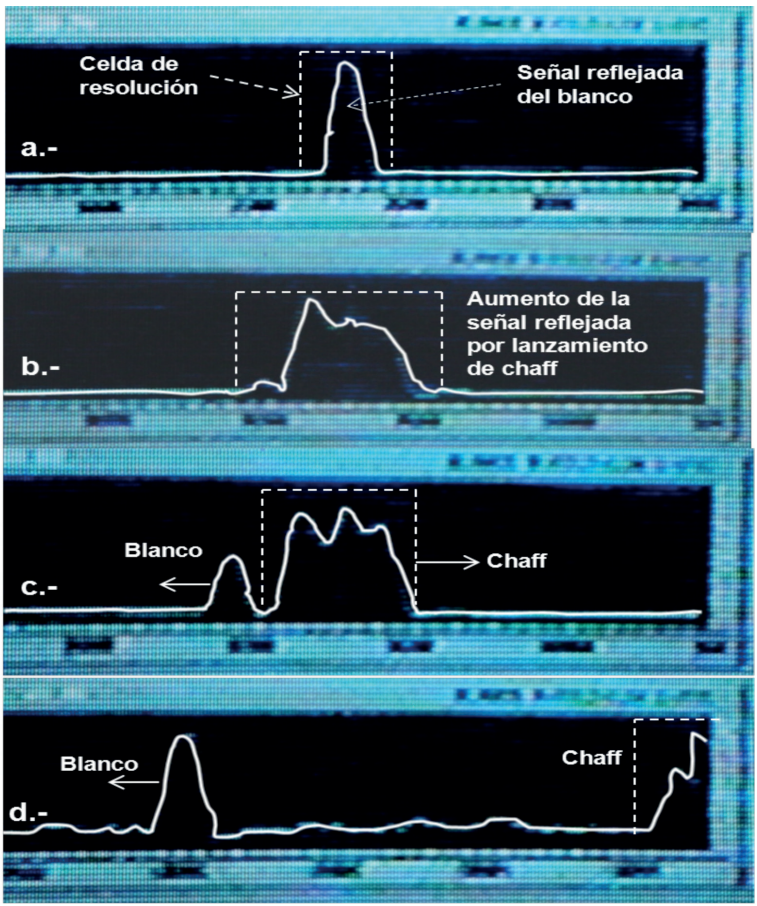

Figura 2.29: Imágenes de la pantalla de un radar de control de fuego en seguimiento de un blanco que lanza *chaff*. Fuente: elaboración propia.

Los buques también utilizan el *chaff* no solo como señuelo de saturación, como se vio en la Figura 2.26, sino que como seducción, principalmente para protegerse contra misiles antibuques guiados por radar. En este caso, la separación de un único señuelo desde el blanco es generada solo por el movimiento del buque y el viento, que moverá la nube de *chaff* y ocasionará que la celda del radar siga el señuelo y pierda al buque.

Capítulo III
Guerra Electrónica de Telecomunicaciones

En este punto se obviará un poco el tema de sensores y las técnicas de *jamming* enfocadas en confundir y evitar los sistemas de armas adversarios. Ahora es el turno de la GE contra las señales de telecomunicaciones.

El ambiente de las telecomunicaciones tácticas es extremadamente denso en el campo de batalla, lo que constituye una importante consideración en todas las actividades de la GE de telecomunicaciones.

Las comunicaciones tácticas son conducidas en rangos de frecuencias HF, VHF y UHF, sin embargo también se deben considerar las señales de comunicaciones de enlaces fijos punto a punto, satelitales y *data links* aire-tierra. La Tabla 3.1 siguiente muestra los usos típicos de enlaces de comunicaciones en cada categoría.

RANGO DE FRECUENCIA	TIPO DE ENLACE	APLICACIÓN MILITAR
HF	Superficie punto a punto	Comunicaciones tácticas de largo alcance para sistemas de mando y control táctico de superficie
VHF / UHF	Aire superficie y aire -aire	Comunicaciones tácticas de superficie en línea de vista, sistemas de mando y control aéreo y de superficie
Microondas	Aire-superficie, repetidores aéreos y satelitales	*Data links* aerotransportados, UAV y sistemas de mando y control aéreos y de superficie

Tabla 3.1: Enlaces de comunicaciones, [9].

En GE existe una práctica común de llamar a las señales asociadas con una amenaza como señal amenaza o simplemente amena-

za. Como se expuso anteriormente, las señales de comunicaciones pueden ser extremadamente amenazantes, por lo que la discusión referida a amenazas de señales de comunicaciones es muy apropiada. Estas incluyen transmisión de comunicaciones de voz y data digital.

La Naturaleza de las Señales de Comunicaciones

Las señales de comunicaciones transportan información desde un lugar hacia otro, por lo que se mueven en una dirección por naturaleza. Sin embargo, la mayoría de las estaciones de comunicaciones tiene transceptores (que transmiten y reciben) permitiendo la propagación en una dirección y en ambos sentidos. Esto es importante para los sistemas de interceptación de comunicaciones debido a que solo el transmisor puede ser localizado.

En general, las señales de comunicaciones tienen modulación continua y tienden a presentar un ciclo de trabajo muy alto, comparado con las señales de radar. Históricamente, las comunicaciones han tomado lugar en los rangos de frecuencia HF, VHF y UHF utilizando modulaciones AM o FM. Sin embargo, con el incremento del uso de los UAV y las comunicaciones satelitales, las señales de comunicaciones del tipo microondas son más comunes. A mayor ancho de banda de la señal, mayor información puede transportar por unidad de tiempo. A mayor frecuencia de la señal, mayor ancho de banda se puede obtener, pero la transmisión es más dependiente de la línea de vista.

A continuación, se exponen dos tipos de señales de comunicaciones importantes como ilustración de las características de las comunicaciones. Estas son las señales de comunicaciones tácticas y las de enlaces digitales o *data links.*

Comunicaciones Tácticas

Las señales de comunicaciones tácticas incluyen comunicaciones superficie-superficie, aire-superficie y aire-aire. Estas señales están en las bandas HF, VHF y UHF y los transceptores tienen antenas con una cobertura de 360° en acimut. Las antenas del tipo látigo son las más comunes en estaciones de comunicaciones basadas en su-

perficie y las antenas tipo dipolo son las más comunes para plataformas aéreas. El empleo de antenas no direccionales permite tener comunicaciones sin saber la localización del otro extremo del enlace. Como las antenas de 360° tienen poca ganancia, puede ser necesario el uso de antenas direccionales para comunicarse entre sitios fijos. Estas antenas proporcionan más ganancia y aislamiento de señales no deseadas [9].

Los transmisores de comunicaciones tácticas tienen desde uno a varios watts de potencia efectiva irradiada (ERP) y los enlaces operan sobre unos pocos kilómetros de distancia. Se debe tener presente que los enlaces HF pueden tener un rango mucho mayor (requiriendo una ERP mayor) debido a la condición de no línea vista de la propagación HF. Las comunicaciones hacia y desde una aeronave en VHF y UHF, también tienen rangos extensos debido a mayores distancias de la línea vista. La información transportada en un enlace de comunicaciones táctico puede ser voz o data y la voz puede ser transportada en formato digital y análogo. La información puede ser encriptada y la señal puede ser de frecuencia fija o protegida de la detección y *homming* (seguimiento por intensidad de señal), por medio de técnicas de "espectro ensanchado" *(spread spectrum)*, siendo la más común de este tipo el salto de frecuencia.

Las comunicaciones tácticas normalmente operan en redes del tipo "presiona y habla" *(push to talk)*, es decir que transmiten a requerimiento. Esta condición involucra varios transceptores operando en la misma frecuencia, con solo una estación transmitiendo a la vez.

Muchos sistemas interceptores de comunicaciones tácticas muestran en sus pantallas relaciones de frecuencia versus ángulo de arribo, según se puede apreciar en la Figura 3.1. En situación de combate, las señales se presentarán aleatoriamente dispersas en acimut y frecuencia, así cada punto en la pantalla representará una transmisión por cada transmisor. Las transmisiones subsecuentes del mismo transmisor mostrarán puntos en la misma frecuencia y ángulo. Una excepción es la señal con salto de frecuencia que tendrá una serie de frecuencias al mismo ángulo de arribo, como lo destaca la Figura 3.1.

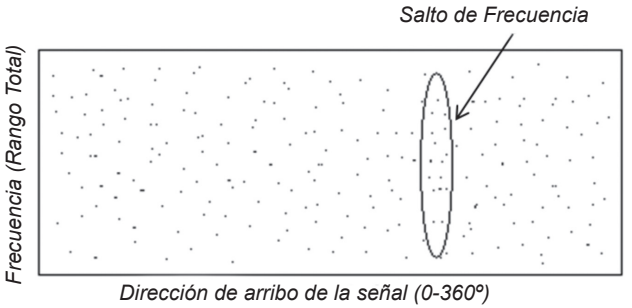

Figura 3.1: Las señales de comunicaciones tácticas vistas por un sistema de interceptación de comunicaciones se dispersan aleatoriamente en frecuencia y ángulo de arribo [3].

Enlaces de Data Digital *(Digital Data Link)*

Los enlaces de data transportan información digital en frecuencias típicamente del tipo microondas. Si se considera un enlace típico entre un UAV y una estación de control, según se muestra en la Figura 3.2, el UAV recibe instrucciones o comandos desde la estación de control y transmite data recolectada a la misma estación. El enlace de control (o *up-link*), usualmente es de banda angosta, debido a que las señales de comando tienden a tener una transmisión de data a una razón relativamente baja. Las señales del *up-link* estarán típicamente encriptadas (para segurizar la información que transmiten) y serán de un alto nivel *spread spectrum* (para proteger los canales de comunicación). Esto protege a la estación de control de la detección y localización que sistemas hostiles puedan ejecutar (sistemas de localización de emisores adversarios), haciendo más difícil interferir el control del UAV.

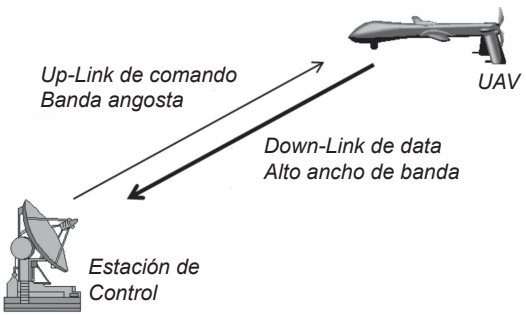

Figura 3.2: Los enlaces entre los UAV y las estaciones de control son *datalinks* digitales típicos. Fuente: elaboración propia.

El enlace del UAV a la estación de control es llamado el *down-link.* También es llamado *data link,* debido a que transporta la data de salida de las cargas útiles del UAV. Tiene un ancho de banda típicamente más amplio que la señal del *up-link* porque transporta una gran cantidad de data. La carga útil más común de los UAV son sistemas de captura de imágenes (televisión o *forward looking infrared* - FLIR) que usualmente requieren millones de bits por segundo para transmisión. Estas señales son típicamente encriptadas y tienen algún nivel de protección del tipo *spread spectrum.* Sin embargo, el amplio ancho de banda para la data transmitida limita la cantidad de esparcimiento en frecuencia que puede aplicarse.

Las antenas del *up-link* tienen un ancho de *beam* o haz del tipo angosto, otorgando directividad al enlace y haciéndolas difícil de interceptar por parte de sistemas de localización de emisores hostiles. Las antenas del *down-link* son limitadas en tamaño debido a las acotadas dimensiones del fuselaje del UAV y a consideraciones aerodinámicas. Por esto, las antenas del *down-link* tienen una ganancia menor y un ancho del haz mayor que las del *up-link* y son principalmente omnidireccionales.

Enlaces Satelitales

Los enlaces satelitales disponen de señales de comunicaciones muy importantes y operan típicamente en frecuencias del tipo microondas, transportando voz y data sobre grandes distancias. La mayoría de los satélites proporcionan acceso a muchos usuarios simultáneamente, por lo tanto sus señales tienen muchos mega Hertz de ancho de banda. Algunos satélites proveen servicios a usuarios comerciales y militares a la vez. Las aplicaciones comerciales típicas incluyen televisión y telefonía. Los satélites militares por otro lado, proporcionan básicamente los mismos servicios, pero los formatos de las señales pueden ser significativamente más diversos, haciendo uso de señales encriptadas si se requiere y pueden complementarse con técnicas *spread spectrum* para protección *anti-jamming.*

Volviendo a las comunicaciones tácticas, la práctica demuestra que la propagación de ondas en el rango de frecuencias correspondiente al HF es muy compleja, sus características varían con la hora durante el día, la estación del año, la localización y las condiciones atmosféricas,

junto a la actividad solar que afectan a la ionósfera. La propagación HF puede ser del tipo línea vista, onda terrestre u onda aérea. La propagación de ondas en el rango VHF y UHF tiene un comportamiento mejor que en el caso del HF. Para las microondas se sabe que requieren de condiciones estrictas de línea vista y de acuerdo a su ancho de banda pueden entregar mayor cantidad de información que las señales HF, VHF y UHF. Este ensayo no pretende profundizar en la descripción de las bandas de comunicaciones, pero prontamente el foco de interés será concentrarse en el ataque electrónico que se pueda llevar en contra de ellas. Por tal razón, a continuación se entrega una breve descripción de las señales de baja probabilidad de interceptación (LPI), particularmente *spread spectrum,* para posteriormente pasar a discutir temas de *jamming* de comunicaciones.

Señales de Baja Probabilidad de Interceptación *(LPI - Low Probability of Intercept)*

Algunas señales de radares como así también algunas señales de comunicaciones tienen características consideradas como LPI. La transmisión de señales LPI tienen alguna combinación de antenas de haz angosto, baja potencia efectiva irradiada y de modulación del tipo espectro ensanchado para hacerlas difíciles de detectar y atacar.

Las señales LPI son un desafío para los sistemas receptores que intentan detectarlas y consideran características que las hacen difíciles de detectar o que hacen difícil la localización de su emisor. La forma más fácil de operar con una señal de este tipo es bajo normas de control de emisión, que consisten en la disminución de la potencia de transmisión a un nivel mínimo que permita a la señal (de radar o de comunicaciones), proveer una adecuada razón S/N, respecto al receptor que la espera. Una menor potencia de transmisión reduce el rango al que cualquier otro receptor adversario pueda detectar la señal transmitida. Otra medida similar es el empleo de antenas de haz angosto o antenas con supresión de lóbulos laterales, que transmiten menos potencia fuera del eje hacia el cual apuntan, de esta forma la señal es más difícil de ser detectada por un receptor hostil. Si la duración de la señal se reduce, el receptor tiene menos tiempo en el cual buscar la señal en frecuencia y/o ángulo de arribo, reduciendo de esta forma su probabilidad de interceptación.

Las señales LPI también reducen su detectabilidad gracias a la modulación aplicada sobre ellas, la que distribuye la energía en un rango de frecuencias mayor al originalmente requerido para transportar la información (ancho de banda de información) de la señal transmitida. Al distribuir la energía en un rango de frecuencia mayor, reduce la intensidad de la señal por ancho de banda de información y como el ruido en un receptor está en función de su ancho de banda de operación, cualquier receptor que intente recibir y procesar esta señal en su ancho de banda total, verá reducida su razón S/N.

Señales *Spread Spectrum* (Espectro Ensanchado)

Como introducción al *jamming* de comunicaciones, las señales *spread spectrum* o de baja probabilidad de interceptación (LPI), distribuyen su energía aleatoriamente sobre un rango de frecuencias más amplio que el requerido con la idea de transportar la información desde el transmisor al receptor. El ancho de banda mínimo requerido para una transmisión de comunicaciones es el ancho de banda de información y el ancho de banda de transmisión es la frecuencia sobre la cual se distribuye la señal. Así, las señales LPI son el resultado del procesamiento de señales electromagnéticas de tal manera que resultan difíciles para el adversario saber si están presentes y si es posible su detección, la información contenida en estas es difícil de extraer.

Para una señal *spread spectrum* se debe disponer de un receptor que tenga la capacidad de reagrupar la señal que es transmitida en un ancho de banda ampliado, para lo cual el receptor debe estar sincronizado con el circuito ensanchador del transmisor, permitiendo al receptor procesar la señal en su condición no ensanchada original. La condición original de la señal comparada con su estado ensanchado puede ser observada en la Figura 3.3. Un receptor adversario no tendrá la capacidad de reagrupar la señal sincronizadamente, por tal razón interceptar, interferir y localizar este tipo de transmisión es altamente complicado. La potencia de ruido en un receptor es proporcional a su ancho de banda efectivo, así el receptor adversario con suficiente ancho de banda como para recibir la señal *spread spectrum,* tendrá una potencia de ruido tan elevada que esconderá la señal *spread spectrum* no permitiendo su interceptación.

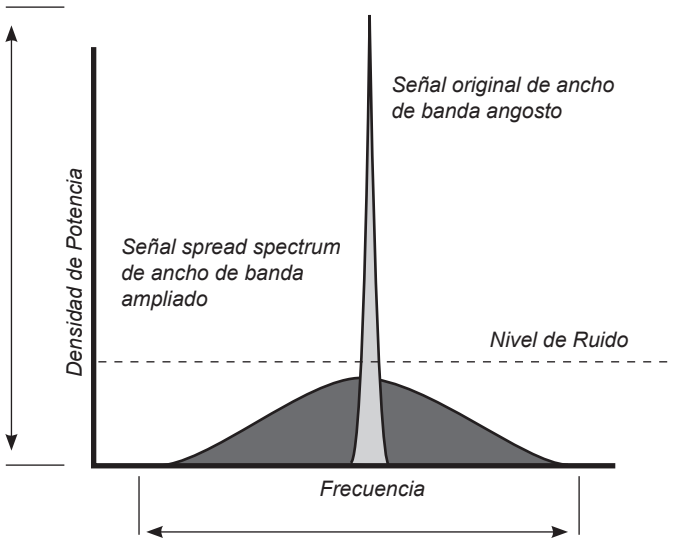

Figura 3.3: Comparación de una señal de transmisión normal con su equivalente en *spread spectrum,* en la que se debe notar el mayor ancho de banda y menor intensidad de señal utilizado. Fuente: elaboración propia.

Las señales *spread spectrum* se pueden clasificar en las siguientes señales, las señales de salto de frecuencia *(frequency hopping)* y las señales secuencia directa *(direct sequence)*. Cada una distribuye la señal original en un ancho de banda mayor, sin embargo la naturaleza de su distribución en potencia versus la frecuencia versus el tiempo para cada tipo de modulación, entrega diferentes vulnerabilidades para ser interceptadas, localizadas e interferidas por *jamming*.

Señales con Salto de Frecuencia *(Frequency Hopping - FH)*

Las señales del tipo FH mueven la señal portadora con la información, periódicamente a frecuencias de transmisión aleatoriamente seleccionadas. El receptor de estos enlaces salta sincronizadamente de frecuencia en frecuencia con el transmisor, así un receptor adversario no sabe la secuencia de saltos. El período de saltos es típicamente inferior a 10 milisegundos y puede ser mucho menor. El FH es una técnica importante para las comunicaciones militares ya que la señal ensanchada puede ser muy amplia en frecuencia. Esta habilidad no es exclusiva de las comunicaciones militares, por el contrario, en el ámbito civil son ampliamente utilizadas

para distintos tipos de enlaces, los que compartiendo una misma banda y colocalización evitan interferencias entre si haciendo uso del FH [9].

Las señales FH constituyen un tipo de señales de baja probabilidad de interceptación (LPI), debido a que el tiempo que estas están presentes al ocupar una frecuencia es tan corto que para un sistema de interceptación es prácticamente imposible detectar la presencia de la señal [7].

Se debe tener presente que las señales FH son una técnica de protección del canal de comunicaciones, por tal razón debe entenderse al FH como una técnica de protección de los enlaces. Varios autores confunden erróneamente su aplicación con técnicas de aseguramiento de la información, cuando el FH actúa sobre el canal o medio de transmisión y no sobre la información en sí misma. Un ejemplo de técnica de aseguramiento de la información es la encriptación, que no tiene nada que ver con la protección del canal de transmisión, pero si actúa directamente sobre la información.

En la siguiente figura se observa una representación gráfica de una señal FH en frecuencia versus tiempo y potencia.

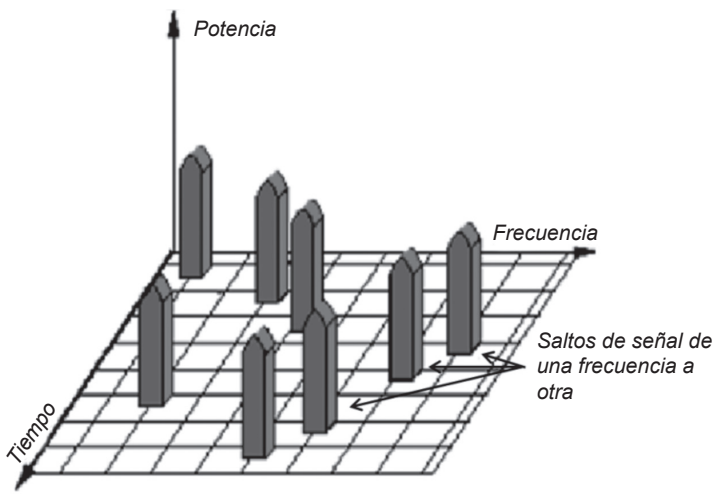

Figura 3.4: Representación de una señal con salto de frecuencia versus tiempo y potencia. Fuente: elaboración propia.

Para poder detectar este tipo de señales cuando su razón de salto es baja, se debe partir de la base que tiene toda su potencia en un ancho de banda de información por un período de 10 milisegundos, para el caso de bajas velocidades de salto. Un receptor puede detectar la presencia de energía en una pequeña parte de este tiempo, así es que puede buscar muchos canales durante cada salto. Aumentar el ancho de banda del receptor ayuda mucho más, porque cubre más frecuencias en cada paso y así avanzar en la búsqueda a una razón mayor. Otra consideración es que no es necesario cubrir toda la banda durante un salto, al capturar un salto ocasional se puede detectar la presencia de la señal. Naturalmente, a mayor razón de salto, más difícil será detectar la señal FH, por tal razón las comunicaciones militares con FH disponen de altas velocidades de salto y normalmente utilizan toda la banda en que operan.

Señales de Secuencia Directa (DS)

Originalmente, la ocupación de una frecuencia que una señal digital hace es proporcional al su taza o razón de bit *(bit rate).* Si una señal digital es modulada una segunda vez con una taza de bit mucho mayor, la energía de la señal se distribuye a lo largo de un rango de frecuencias proporcionalmente mucho mayor. Este proceso es llamado modulación de espectro ensanchado del tipo secuencia directa *(direct sequence spread spectrum - DSSS).* Un ejemplo es la aplicación de una señal llamada chip, que es sumada a la señal original antes de ser transmitida (ver Figura 3.5). La secuencia chip es una señal digital que cambia los estados de los bits a una razón mucho mayor que la señal de información. El efecto en el enlace es que la señal resultante es mucho más ancha en frecuencia y a cualquier frecuencia en particular resulta ser mucho más baja en amplitud, ya que la misma potencia de la señal está presente, pero se extiende a lo largo de un rango de frecuencia mayor o más ancho. Esa señal de amplitud tan baja resulta difícil de ser detectada si no se sabe que está presente.

La baja probabilidad de intercepción (LPI) de una señal del tipo DS se sustenta en que cualquier receptor no compatible de ancho de banda lo suficiente amplio como para recibir la señal, tendrá tanto ruido de fondo que la razón de señal a ruido de la señal interceptada será muy baja. Esto es lo que caracteriza a las señales DS cuyo nivel se

mantiene por debajo del ruido, dándole la condición de baja probabilidad de interceptación [7].

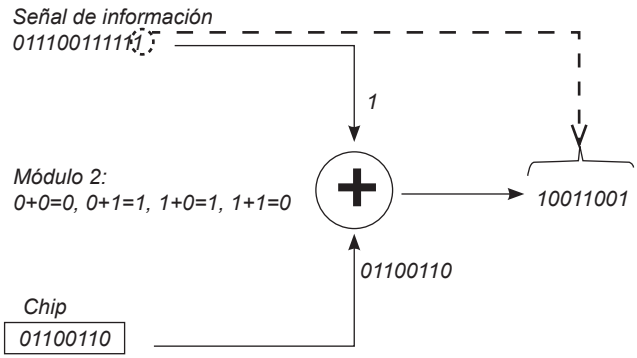

Figura 3.5: Representación de una señal de información transformada en *direct sequence* por medio de la adición en módulo dos. Cada bit es sumado con el chip, pasando a ser representado en 8 bits según la secuencia del chip.
Fuente: elaboración propia.

La interceptación de señales *spread spectrum* como las DS, requieren equipos receptores de un mayor ancho de banda también. Desafortunadamente hay una ley de la física que establece que a mayor ancho de banda del equipo de recepción, mayor será el ruido de fondo que entra al receptor junto a cualquier señal deseada, por lo tanto en la medida que los sistemas de inteligencia de señales amplíen su ancho de banda en la búsqueda, se saturarán con mayor facilidad, lo que dificultará la interceptación de este tipo de señales, según se representa en la próxima figura:

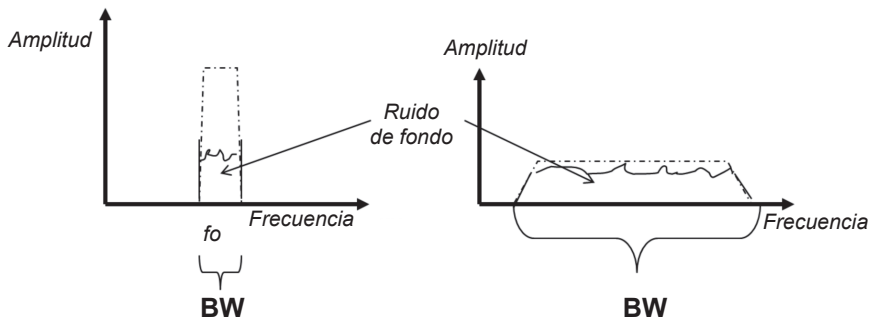

Figura 3.6: Comparación del nivel de ruido de una señal normal versus una señal con la misma información, pero del tipo DSSS. Fuente: elaboración propia.

Jamming de Comunicaciones

El objetivo del *jamming* de comunicaciones es interferir las comunicaciones del adversario por medio de la irradiación de una mayor potencia hacia el receptor en la red en el que se encuentra el transmisor adversario [8].

Al concentrar la discusión en interferir señales de comunicaciones, dejando de lado las señales de radar, la primera de las diferencias entre ambas es la geometría de la ejecución de la interferencia. Mientras un radar tiene tanto el transmisor como el receptor en la misma ubicación (generalmente), un enlace de comunicaciones siempre tiene un transmisor en una localización distinta a la del receptor. Se debe tener presente que la interferencia es contra el receptor y aunque en comunicaciones se utilice transceptores, solo se atacará al receptor. Por esto, si en un enlace se tiene dos puntos que están en comunicación bidireccional, para que el *jamming* pueda interferir a ambos puntos, se debe transmitir un *jamming* a un nivel de potencia tal que llegue con suficiente intensidad a ambas posiciones como para lograr una razón J/S superior a 1 en ambas, esta condición es representada en la Figura 3.7. Por tal razón, el *jammer* normalmente es muy móvil y no permanece en la misma posición por mucho tiempo después de haber operado contra un enlace. Los *jammers* de superficie operan principalmente en parejas, uno transmite mientras el otro se está moviendo. De esta forma se puede lograr un *jamming* continuo, minimizando la posibilidad de detección.

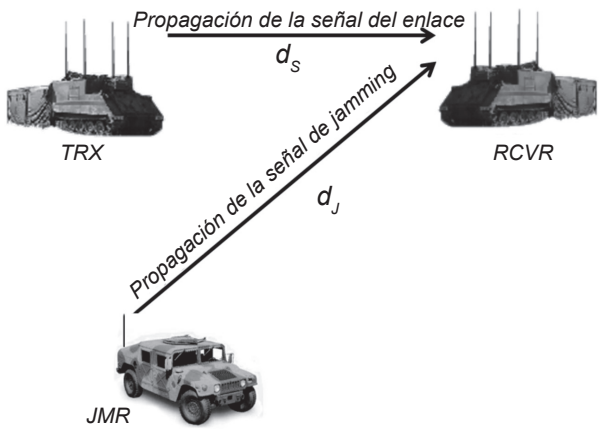

Figura 3.7: Geometría del *jamming* de comunicaciones, tanto la señal de comunicación como del *jamming* van en el mismo sentido hacia el receptor [8].

El *jamming* puede ser utilizado para atacar sistemas de comunicaciones adversarios o sus capacidades de apoyo electrónico también. El *jamming* utilizado para reducir la efectividad del apoyo electrónico adversario es conocido como enmascaramiento. El uso del enmascaramiento permite a los sistemas de comunicaciones propios operar con un riesgo reducido del apoyo electrónico adversario. Cabe hacer presente que el *jamming* se utiliza contra receptores de RF (radio-frecuencia).

Existen algunos casos importantes en donde no se utilizan transceptores, por ejemplo en los enlaces de UAV de la Figura 3.8. En esta figura se observa el jamming sobre el *data-link* (o *down-link*), reafirmando que la interferencia es contra el receptor, que en este caso se encuentra en tierra.

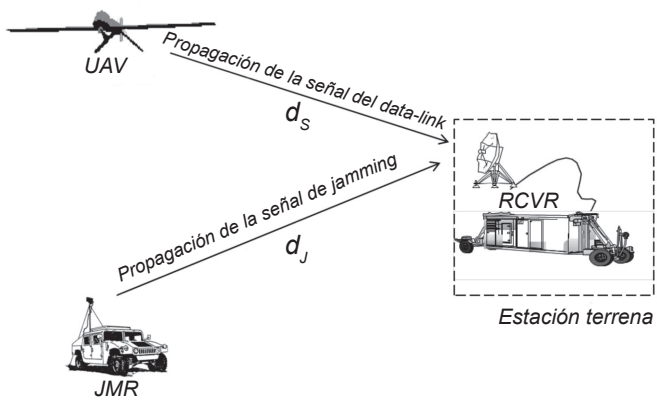

Figura 3.8: Un *jammer* atacando un *data-link* de UAV. El *jamming* es contra el receptor de la estación terrena. Fuente: elaboración propia.

Otra diferencia importante con el *jamming* de radares es que las señales de radar hacen un viaje de ida y vuelta al blanco, por lo tanto la señal recibida es inversamente proporcional a la distancia al blanco y es determinada por $1/R^4$. Como la potencia del *jammer* se transmite solo en un sentido, solo se reduce por el cuadrado de la distancia ($1/R^2$). En *jamming* de comunicaciones, tanto la potencia de la señal transmitida y la potencia del *jammer* se reducen por el cuadrado de sus respectivas distancias.

La razón *jamming* a señal es representada por la siguiente ecuación:

$$\frac{J}{S} = \frac{(ERP_J)(G_{RJ})(d_S^2)}{(ERP_S)(G_R)(d_J^2)}$$

, donde ERP_J es la potencia efectiva irradiada por el *jammer*; ERP_S es la potencia efectiva irradiada del transmisor; d_J es la distancia del *jammer* al receptor; d_S es la distancia desde el transmisor al receptor; G_{RJ} es la ganancia de la antena receptora hacia el jammer; G_R es la ganancia de la antena receptora hacia el transmisor. Esta ecuación puede ser pasada a una notación en decibeles y queda de la siguiente forma:

$$J/S = ERP_J - ERP_S + 20\log(d_S) - 20\log(d_J) + G_{RJ} - G_R$$

Los elementos de esta fórmula son los mismos a los anteriores, pero las ERP se encuentran en unidades de dBm o dBw y las ganancias en dB. En ambas ecuaciones, las ERP son el producto (o suma en la ecuación en dB) de la potencia de salida del transmisor y la ganancia de la antena en la dirección del receptor.

En comunicaciones tácticas, donde todos los participantes utilizan transceptores con antenas tipo látigo, la ganancia de la antena del receptor es simétrica en acimut, por lo que la ganancia hacia el *jammer* será la a misma que la ganancia hacia el transmisor, por lo que ambos términos terminan anulándose en la ecuación.

Cuando se interfieren señales de comunicaciones de modulación análoga, es normalmente necesario alcanzar un valor superior a 1 en la razón J/S. Esto es necesario porque un operador en el receptor puede tener la habilidad suficiente como para escuchar la comunicación adaptivamente, es decir puede tener un oído entrenado como para extraer información del enlace a pesar de la existencia de ruido en este. En comunicaciones de voz y video análogo de baja calidad de transmisión, se pueden rellenar los tramos que resulten con mucho ruido siguiendo el contexto del mensaje o la información. Esto es real en comunicaciones militares tácticas, donde la información importante es enviada en formatos muy rígidos. Ejemplo de estos son el lenguaje convenido, el alfabeto fonético y el código Q en el caso de comunicaciones civiles.

Cuando se interfieren señales de comunicaciones moduladas digitalmente, el ataque debe lograr que la señal recibida sea ilegible para el demodulador digital del receptor, para eso se puede interferir la

sincronización o producir bit erróneos, pero como la sincronización tiende a ser muy robusta, la forma más básica de atacar estos enlaces es incrementando los bit erróneos. En términos generales, la señal recibida no se reduce mucho más por una J/S con valores mayores a uno, si no que bastará que la señal sea ilegible solo una tercera parte del tiempo, así será considerada inútil. Un ejemplo práctico de cuando ocurre esto es cuando una radio con salto de frecuencia encuentra que una tercera parte de los canales sobre los que salta están ocupados por señales fuertes, así el enlace no se concretará. Esto significa que una señal digital solo necesita ser jammeada a una razón J/S de 0 dB durante una tercera parte del tiempo, mientras que una señal análoga requiere una razón J/S positiva durante el 100% del tiempo.

Jamming contra Señales *Spread Spectrum*

Las señales de espectro ensanchado están sujetas a las mismas ecuaciones de *jamming* que cualquier otra señal, pero la habilidad del receptor cooperativo para trabajar con un espectro colapsado le da una ganancia de procesamiento que reduce la efectividad del *jamming*. En general, la ventaja de la ganancia de procesamiento es la misma que la razón de ensanchamiento (el ancho de banda de transmisión/ el ancho de banda de información).

Jamming contra Señales *Frequency Hopping* (FH)

Los sistemas de comunicaciones con capacidad FH se dice que tienen una capacidad *anti-jamming*, esta ventaja se basa en que el *jammer* solo conoce el rango de salto total y debe repartir su potencia de transmisión sobre la totalidad de ese rango de frecuencias.

Si una señal de *jamming* de ancho de banda angosto se aplica contra un receptor del tipo salto de frecuencia, el *jamming* será efectivo solo cuando el receptor salte en la misma frecuencia en que transmite el *jammer*. Esto causará que la efectividad del *jamming* sea significativamente baja. Por tal razón se requieren equipos de *jamming* sofisticados para interferir señales con salto de frecuencia. Para el caso de señales FH de baja velocidad de salto, la señal permanece en una frecuencia solo por un período de salto, el sistema de *jamming* necesita determinar la frecuencia de transmisión y aplicar *jamming* al receptor víctima por el tiempo suficientemente necesario del período del salto para así evitar

una comunicación exitosa. Cómo ya se vio anteriormente, las señales digitales necesitan ser interferidas con *jamming* solo un 33% del tiempo con una razón J/S de 0 dB. Esto significa que la señal FH de *jamming* requiere una potencia moderada, si el *jammer* tiene una capacidad de recepción y procesamiento que puede detectar la frecuencia FH y activar la transmisión del *jammer* en menos del 57% del período de saltos.

Un *jammer* que interfiere cada salto se llama "jammer de seguimiento", que requiere de subsistemas receptores y procesadores muy complejos, disponibles como estado del arte en la tecnología actual y que permiten la rápida medición de la frecuencia detectada, a la vez que aplican la potencia de transmisión del *jammer* sobre esa señal lo suficientemente rápido para negar al adversario la posibilidad de transmitir información en cada salto.

Otra forma de interferir una señal con salto de frecuencia es por medio de la interferencia parcial de la banda de operación. Con esta técnica es necesario determinar el ancho de banda que cubre la señal y el nivel de señal deseado a la entrada del receptor, con estos datos la potencia del *jammer* se distribuye sobre el máximo del rango de frecuencias, esto asume que se dispone de potencia suficiente en el *jammer* para igualar la potencia de la señal deseada en el receptor en cada salto de frecuencia, sin embargo una desventaja de este tipo de *jammer* es que lo más probable es que cometa fratricidio al interferir paralelamente enlaces de comunicaciones amigas que operan en el mismo rango de frecuencias. Para superar este problema se debe posicionar el *jammer* lo más cercano posible al receptor adversario, lo que permite una interferencia efectiva con un mínimo de potencia y proteger las comunicaciones amigas. Este método de empleo del *jammer* será efectivo contra cualquier modo de comunicación *spread spectrum*.

Como se puede ver en la Figura 3.9, si se conoce la ubicación del transmisor de la señal esperada, la medición de la intensidad de la señal en el receptor del *jammer* permitirá el cálculo de la ERP. Se asume que el transmisor tiene una antena del tipo látigo u otro tipo con cobertura de 360° en acimut. El problema es más complejo cuando el enlace interferido utiliza antenas direccionales, pero también tiene solución. La ERP del transmisor de la señal esperada es la intensidad de la señal (ajustada para la ganancia de la antena del receptor del *jammer*) ponderada por las pérdidas de propagación según la siguiente fórmula:

$$ERP_S = P_{RJ} - G_{RJ} + 32 + 20\log F + 20\log d_{TJ}$$

, donde ERP_S es la potencia efectiva irradiada del transmisor de la señal deseada en dBm; P_{RJ} es la potencia recibida en el receptor del jammer en dB; G_{RJ} es la ganancia de la antena receptora del *jammer* en dB; F es la frecuencia de la señal deseada en MHz y d_{TJ} es la distancia desde el transmisor de la señal esperada al *jammer*.

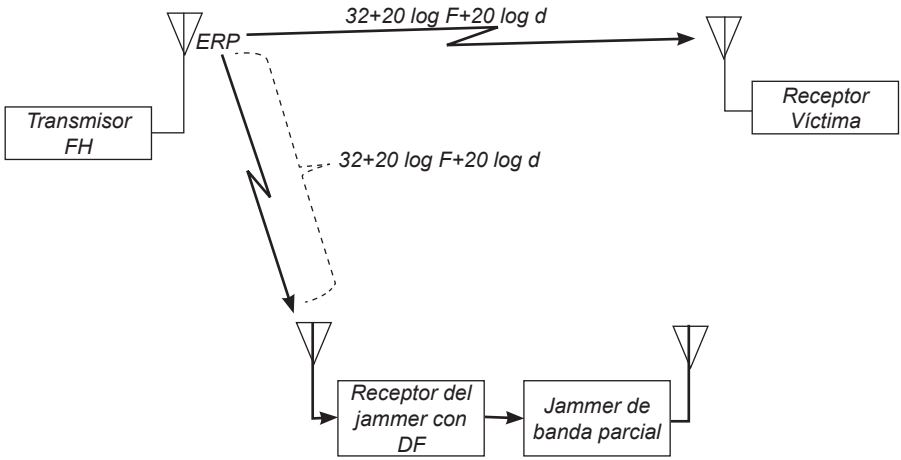

Figura 3.9: Si se conoce la localización del transmisor, el receptor del *jammer* puede determinar la ERP del transmisor desde la potencia de la señal recibida [3].

La ERP_S calculada puede ser ajustada por pérdidas atmosféricas y cualquier condición física conocida tal como lluvia y directividad de la antena transmisora si corresponde, sin embargo las pérdidas de propagación serán el factor primario de las pérdidas. Ahora, si el enlace de comunicaciones a *jammear* utiliza transceptores, la localización del receptor a ser interferido puede ser determinada y con esa localización, es posible calcular la distancia desde el transmisor del enlace hacia el receptor víctima. Entonces, la potencia de la señal recibida a la entrada del receptor víctima puede ser calculada usando la fórmula de pérdidas de espacio libre:

$$L_S = 32 + 20\log F + 20\log d$$

Como se muestra en la Figura 3.10, la ERP requerida del *jammer* para alcanzar una razón J/S de 0 dB (dónde la potencia recibida del *jammer* es igual a la potencia recibida de la señal esperada, en la entrada del

receptor víctima), puede ser calculada con la información de distancia entre el *jammer* y el receptor víctima, a cualquier frecuencia en el rango de saltos del enlace. Entonces, la potencia total de salida del transmisor del *jammer* se distribuye sobre el máximo de frecuencias de la banda y así el transmisor alcanzará esa potencia en cada salto. Si el *jammer* puede cubrir un tercio de los canales sobre los cuales la señal deseada salta, el *jamming* es considerado efectivo, así aunque el *jammer* no cubra la totalidad de los canales, el *jamming* de banda parcial optimiza la efectividad del *jamming*. Esta cualidad es muy relevante porque un *jammer* de banda parcial no requiere de un receptor sofisticado capaz de detectar rápidamente la frecuencia de cada salto.

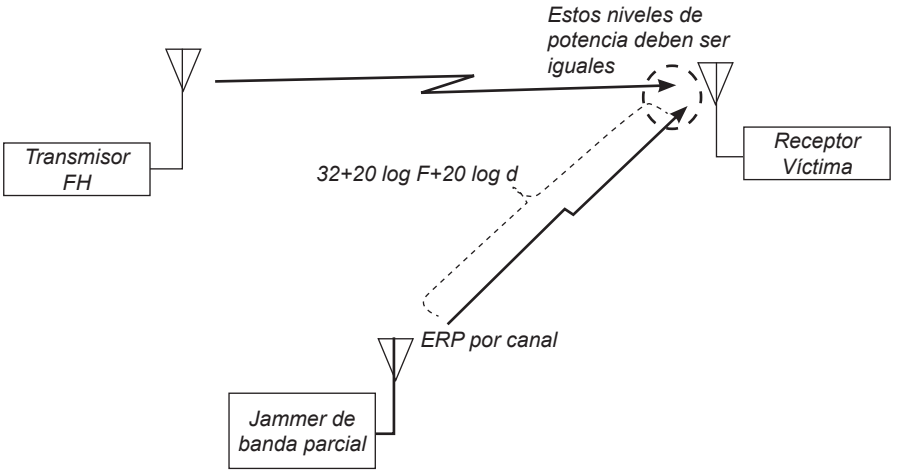

Figura 3.10: La ERP del *jammer* por canal debe entregar una señal en la antena del receptor víctima de igual potencia que la señal que llega del enlace [3].

Señales de *Jamming*

Una señal de *jamming* es creada por la modulación de una señal banda base sobre el canal a ser jammeado. Las señales de *jamming* más comunes son ruido modulado en frecuencia, ruido modulado en amplitud y CW.

El ruido modulado en frecuencia puede ser utilizado para atacar transmisiones moduladas tanto en frecuencia como en amplitud. El ancho de banda de la señal de *jamming* es controlado por una combinación del ancho de banda de la señal banda base y el índice de modulación del modulador de frecuencia. Una señal de *jamming* de ruido modula-

do en frecuencia lo suficientemente fuerte, capturará un receptor FM, evitando que la señal original sea recibida. Una señal de *jamming* de ruido modulado en frecuencia más débil incrementará la taza de bit erróneo en los sistemas de transferencia de data e incrementará parcialmente el ruido en los sistemas de voz FM. La señal de *jamming* de ruido modulado en frecuencia adicionará ruido en un receptor AM, causando niveles significativos de degradación de la señal.

El ruido modulado en amplitud puede ser utilizado en forma efectiva solo contra señales de transmisión AM. El ruido modulado en amplitud tiene muy poco impacto sobre las transmisiones en FM, a no ser que el nivel de ruido sea considerablemente grande. El impacto de una señal de *jamming* de ruido modulado en amplitud sobre una transmisión AM será incrementar el ruido en el receptor.

El *jamming* de CW involucra transmitir solo una señal portadora. Este *jamming* puede ser efectivo contra transmisiones de modulación en frecuencia y contra transmisiones AM, cuando su nivel de señal es mucho más grande que la misma transmisión. El inconveniente del *jamming* CW es que es predecible, lo que lo hace más fácil de superar por técnicas de protección electrónica.

Tipos de *Jamming* de Comunicaciones

Existe un número de diferentes tipos de *jamming* de comunicaciones que pueden ser empleados. Los principales tipos y sus características son presentados en la Figura 3.11.

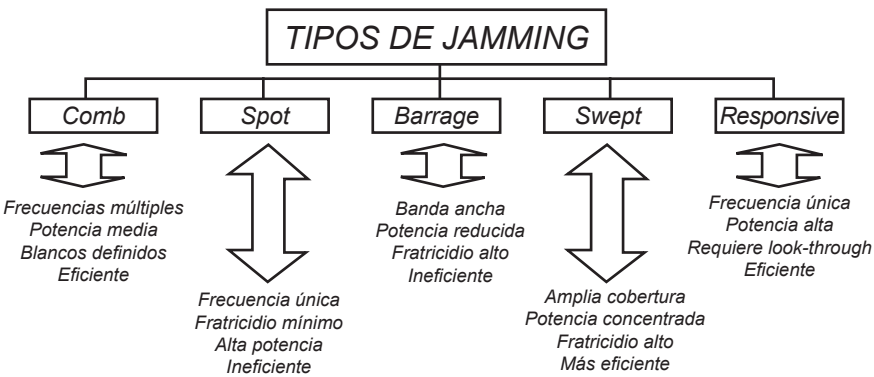

Figura 3.11: Tipos de *jamming* de comunicaciones, [1].

El *Spot Jamming*

El *spot jamming* ocurre sobre un único canal. Como se ve en la Figura 3.12, un *spot jammer* consiste de un generador para la señal *jamming*, un transmisor que traslada la señal *jamming* desde la banda base al canal que será jammeado y se difiere de un transmisor de comunicaciones solo en su potencia de salida que es mayor y una antena que usualmente es direccional.

El generador para la señal de *jamming* produce una señal en banda base que usualmente es ruido. El transmisor modula la señal en banda base, poniéndola en el canal a ser jammeado. Esta modulación puede ser FM o AM. El ancho de banda de la señal transmitida usualmente será el mismo ancho de banda del canal del sistema víctima. Los transmisores también tienen amplificadores de potencia. La antena direccional debe ser apuntada hacia el receptor víctima. El empleo de antenas direccionales aumenta la potencia del *jammer* en el receptor víctima y minimiza la potencia del mismo *jammer* en otras direcciones que pueden impactar sistemas de comunicaciones amigas.

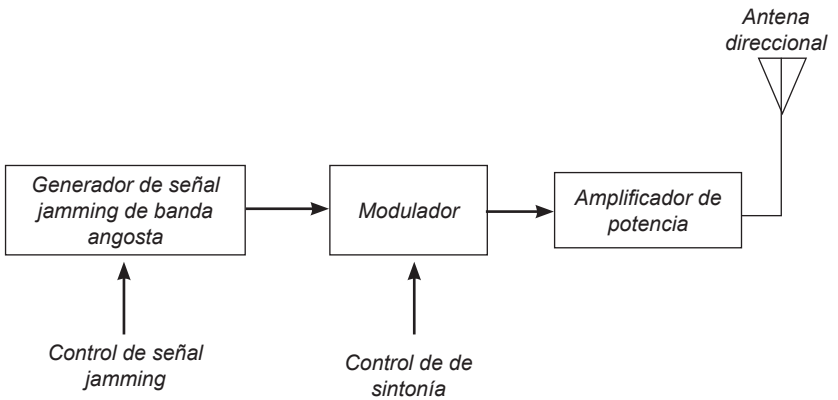

Figura 3.12: Estructura de un *spot jammer* [3].

El *spot jammer* tiene la ventaja que toda la potencia del *jamming* se concentra en un solo canal, que maximizará el impacto del *jamming* sobre un receptor sintonizado a ese canal. El *jamming* contra un solo canal también minimiza el fratricidio, ya que los sistemas de comunicaciones amigas que utilizan otros canales no serán afectados por el *jamming*.

Las desventajas del *spot jammer* son la falta de flexibilidad, el nivel de control requerido y la falta de un método para proveer la capacidad de cambiar ágilmente de canal para jammear. El *spot jammer* se sintoniza en un solo canal así como lo hace cualquier transmisor como se puede ver en la Figura 3.13, pero no puede cambiar rápidamente de canal. Cuando se usa un *spot jammer,* la interferencia debe ser periódicamente suspendida por cortos lapsos para permitir al apoyo electrónico amigo y evaluar su efectividad. Este requerimiento puede ser obviado si el receptor del equipo de apoyo electrónico (o COMINT), se encuentra muy alejado del *jammer* de tal forma que su receptor no sea saturado por la alta potencia de la señal del *jammer*.

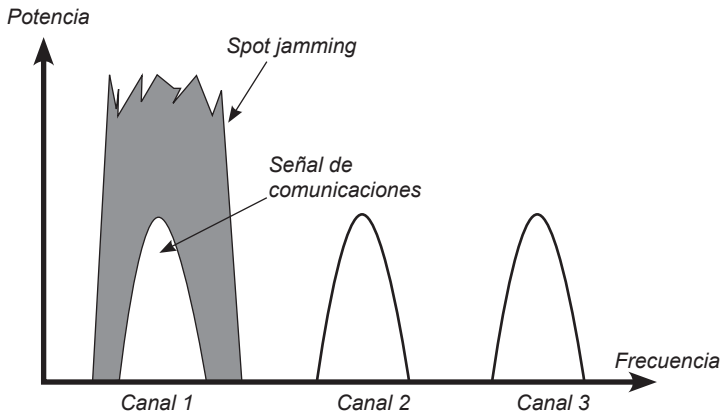

Figura 3.13: El *spot jammer* puede atacar solo un canal a la vez. Fuente: elaboración propia.

Barrage Jamming o *Jamming* de Barrera

En este caso la señal de *jamming* se distribuye a lo largo de un gran número de canales adyacentes. Como interfiere un gran número de canales, un *jammer* de barrera requiere al menos un poco de información acerca de las frecuencias utilizadas por el sistema de comunicaciones adversario. Su potencia se distribuye a lo largo de un número de canales, reduciendo la potencia del *jammer* en cada uno de estos al compararlo con un *spot jammer,* así el impacto de este tipo de *jammer* es más reducido.

Un *jammer* de barrera como el de la Figura 3.14, consiste en un generador para la señal *jamming*, un transmisor que entrega modulación y amplificación de potencia y una antena direccional.

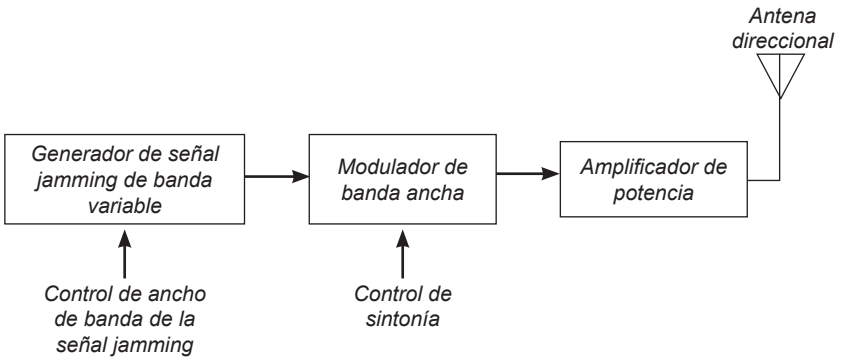

Figura 3.14: Estructura del *barrage jammer* [3].

El generador produce una señal en banda base para la señal de *jamming*, que usualmente es el ruido para el *jammer* de barrera. Paralelamente se le provee un medio para ajustar el ancho de banda de la señal de *jamming* transmitida. Esto puede involucrar un proceso de control de la modulación o el ancho de banda de la señal *jamming* en banda base.

Para prevenir el fratricidio, el empleo de una antena direccional con un *barrage jammer* es más importante que con un *spot jammer.* La potencia de salida en cada canal es más baja que en un *spot jammer,* reduciendo el impacto en las comunicaciones adversarias, según se puede observar en la Figura 3.15. Como se interfiere un gran número de canales, probablemente el impacto sobre las comunicaciones amigas es mayor. Así el empleo de antenas direccionales dará alguna protección a las comunicaciones amigas reduciendo la potencia de *jamming* transmitida en otras direcciones.

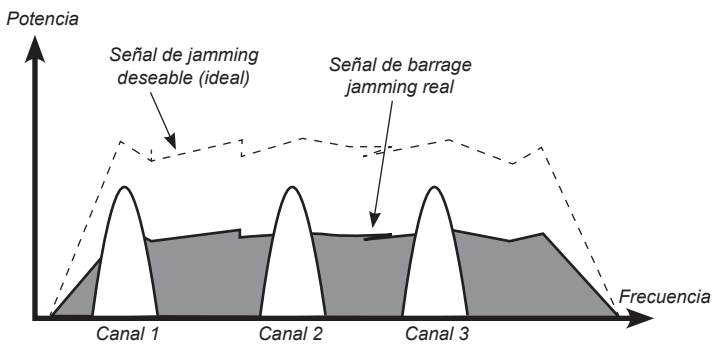

Figura 3.15: El *barrage jammer* transmite un nivel de señal para cada canal, pero es de menor intensidad que en el caso del *spot jammer*. Fuente: elaboración propia.

La evaluación de la efectividad del *barrage jamming* puede requerir una suspensión periódica del *jamming* para permitir operar al apoyo electrónico amigo. Un *barrage jammer* es más fácil de construir que un transmisor de comunicaciones con el mismo ancho de banda y potencia, debido a que la calidad de la señal transmitida no es importante.

Swept Jamming o *Jamming* de Barrido

Este tipo de *jammer* consiste en una fuente en banda base para la señal *jamming*, un transmisor cuya frecuencia de salida es capaz de desplazarse a lo largo de una banda específica y una antena, según se muestra en la Figura 3.16. Como un *barrage jammer,* el *swept jammer* opera sobre un número de canales adyacentes y emplea una antena direccional para evitar el fratricidio. A diferencia del *barrage jammer*, el *swept jammer* se desplaza sobre el ancho de banda determinado y va interfiriendo canal por canal a una razón (velocidad) determinada, que puede ser programada lo que como resultado entrega una suerte de *spot jammer* que se desplaza sobre un ancho de banda, atacando canal por canal, generando una recepción de ruido intermitente en los sistemas de comunicaciones adversarios.

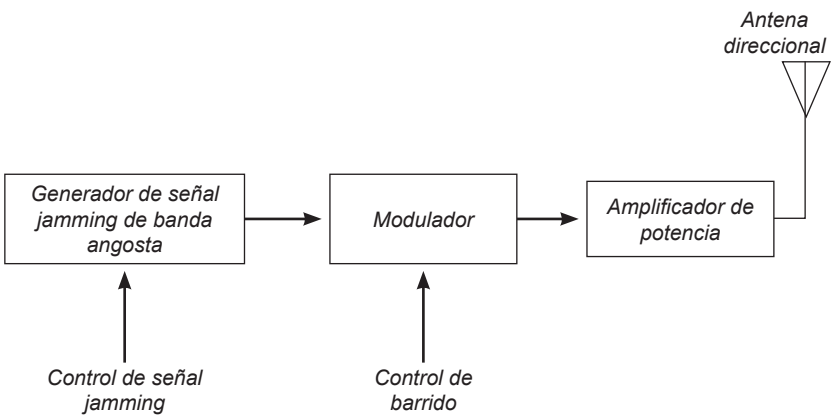

Figura 3.16: Estructura de un *swept jammer* [3].

En algunas ocasiones puede ser factible evaluar el impacto del *swept jamming* sobre los sistemas de comunicaciones adversarios sin suspender el *jamming*. Como el *swept jammer* interfiere un solo canal a la vez, los sistemas de apoyo electrónico pueden monitorear los canales durante el período en que estos no son interferidos. Esto requiere una coordinación

de detalle entre los componentes del ataque y del apoyo electrónico y su dificultad se incrementa con la razón de barrido del *swept jammer.*

Un *swept jammer* tiene la probabilidad de ser más efectivo que el *barrage jammer* debido a que concentra toda la potencia transmitida en un canal, barriendo la frecuencia de esos canales a lo largo de la banda en que se encuentran, según se puede ver en la Figura 3.17. El impacto del *swept jamming* es mayor sobre redes encriptadas, donde el *jamming* puede causar la pérdida de sincronización en los sistemas de desencriptación, incluso si el *jammer* deja de transmitir, la transmisión de data no puede llevarse a acabo de forma inmediata hasta que se readquiera el sincronismo requerido.

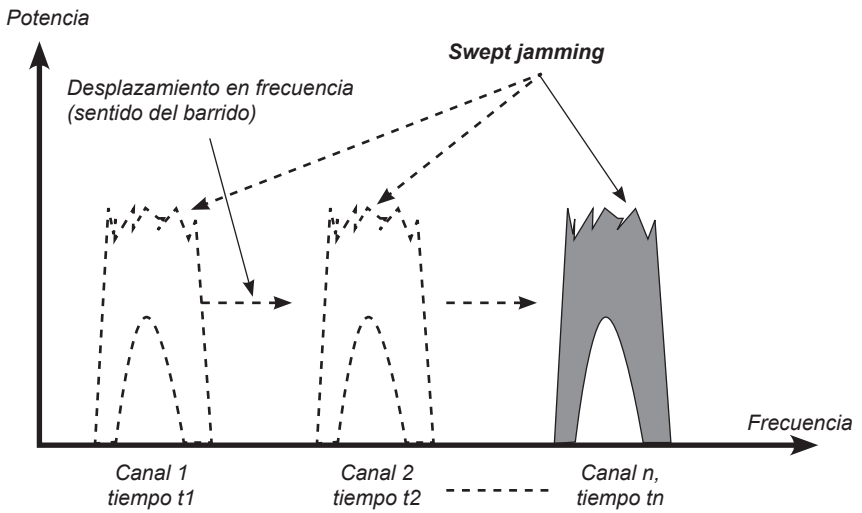

Figura 3.17: El *swept jammer* concentra toda la potencia transmitida en un solo canal a la vez, pero va barriendo en frecuencia los canales adyacentes contenidos en una banda. Fuente: elaboración propia.

Comb Jamming

Un *comb jammer* permite jammear varios canales. Esos canales pueden ser individualmente seleccionados por el operador o pueden tener un intervalo fijo. El *jammer* transmite simultáneamente en todos los canales y al igual que en los casos anteriores, el empleo de una antena direccional disminuye la interferencia sobre los sistemas de comunicaciones propios [1].

El *comb jammer* tiene mayor flexibilidad que el *spot jammer* debido a que permite interferir más de un canal a la vez. La potencia aplicada a cada uno de esos canales es reducida porque la potencia disponible debe compartirse entre el número total de canales que se pretende atacar, sin embargo la eficiencia es mayor que en el caso del *barrage jammer* ya que el *comb jammer* selecciona los canales en vez de interferir toda la banda.

Responsive Jammer o *Jammer* de Seguimiento

Este *jammer* es del tipo *spot* (opera contra un solo canal a la vez), pero ataca cuando detecta una transmisión. Un *responsive jammer* consiste de un receptor de búsqueda, un generador para la señal víctima, un transmisor para modular la señal *jamming*, una antena y una unidad de control como se puede ver en la Figura 3.18**.** El receptor de búsqueda es utilizado para detectar las transmisiones que serán interferidas con el *jammer*. Las frecuencias que serán interferidas son programadas en la unidad de control, así cuando una transmisión es detectada, la unidad de control enciende el *jamming* por un período específico. Periódicamente, la unidad de control dejará de transmitir la señal *jamming* por un corto período (llamado *look-through,* que quiere decir mirar a través), durante el cual el receptor de búsqueda determinará si la transmisión adversaria sigue activa. Si la transmisión sigue activa, el *jammer* reiniciará la interferencia. El período *look-through* puede ser del orden de 40 ms aproximadamente.

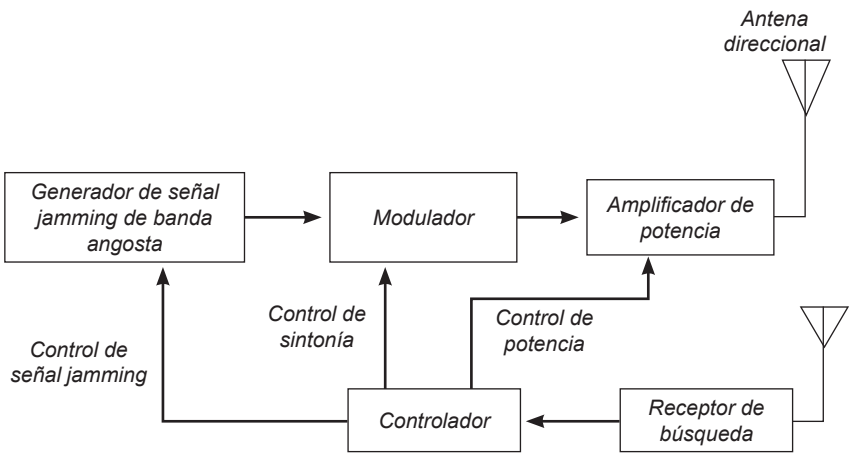

Figura 3.18: Estructura de un *responsive jammer* [3].

La antena utilizada por un *responsive jammer* puede ser omnidireccional o direccional, para cuando la posición del receptor víctima sea fija y conocida. Un *responsive jammer* tiene todas las ventajas de un *spot jammer,* pero tiene la ventaja adicional de la flexibilidad ya que su unidad de control puede ser programada con un número de frecuencias a ser interferidas. El *responsive jammer* reduce el consumo de potencia ya que transmite solo cuando hay una señal para ser jammeada, de esta forma se reduce el peso y tamaño de las baterías requeridas en aplicaciones portátiles y también reduce su firma electromagnética, incrementando la dificultad para un adversario de encontrarlo y neutralizarlo. Este tipo de *jammer* puede incluir dispositivos que le permitan operar como parte de una red automática de *jammers* en que solo uno de ellos estará activo sobre un canal específico a la vez, disminuyendo la firma individual de todos los *jammers* de la red. Un *responsive jammer* típico y moderno permite ingresar en su programación una lista de frecuencias adversarias priorizadas, con el objetivo de buscar esas frecuencias partiendo por las de mayor prioridad, hasta que una transmisión sea detectada. Entonces esa transmisión será interferida por un período preprogramado. Durante el *look-through,* el *jammer* volverá a buscar las frecuencias priorizadas y si detecta una transmisión de mayor prioridad, el *jammer* se cambiará de canal para interferir esa nueva señal.

Pareciera ser que un *jammer* del tipo *responsive* es la solución ideal como técnica y equipamiento de ataque electrónico en comunicaciones, sin embargo el desarrollo de los *jammers* ha demostrado que con el incremento en la razón de saltos de frecuencia que un enlace puede tener hoy, la etapa de recepción y los procesadores de los *jammers* no son lo suficientemente rápidos como para lograr transmitir su señal y afectar ese tipo de enlaces. Por esto, para lograr interferir un sistema de comunicaciones moderno, aparte de contar con el equipo de *jamming* adecuado se requiere la inteligencia de señales pertinente, que pueda entregar la mayor cantidad de parámetros de sus enlaces.

Factores Operacionales

Debe considerarse que sin una cuidadosa planificación y control de los recursos de *jamming* existe un riesgo inherente de fratricidio contra las capacidades de comunicaciones, de vigilancia y de intercep-

tación amigas. Sin embargo, para ser efectivo, el *jamming* debe ser comprensivo, por ejemplo, para negar la totalidad de las comunicaciones a un comandante adversario, se debe atacar simultáneamente todos los sistemas HF, VHF y repetidores de señales de radio en un plan de ataque. Por esto, existen algunos factores operacionales que deben ser considerados antes de tomar la decisión de jammear al adversario:

Inteligencia: Normalmente será menos valioso negar al adversario el empleo del EEM que monitorearlo para obtener inteligencia.

Alternativas: El ataque electrónico es un sistema de armas disponible. Otras formas de ataque, como la artillería o los aviones de ataque a tierra pueden ser más efectivos, sin embargo el efecto sobre el blanco debe ser cuidadosamente considerado antes de seleccionar el método de ataque.

Seguridad: El *jamming* puede alertar al adversario que ha perdido el empleo que hace del EEM, lo que motivará el cambio de sus frecuencias de operación y tendrán que ser detectadas nuevamente. En ciertos casos muy sensibles, la habilidad de interceptar y monitorear las comunicaciones adversarias es tan crítica que el *jamming* nunca puede ser considerado por temor a ceder esa capacidad. El *jamming* también puede delatar la ejecución de futuras intenciones y/o acciones, tales como predecir la incursión de un grupo de ataque.

Tiempo: Así como el fuego de apoyo, el *jamming* debe ser ajustado en el tiempo para presentarse en el momento apropiado de la batalla.

Selectividad: Las capacidades de GE son escasas y se necesita que sean empleadas efectivamente. Por lo tanto son controladas al nivel más alto y tienen procedimientos y doctrinas completas asociadas.

Capítulo IV
Protección Electrónica

El *jamming* impacta de diferente forma a los subsistemas de comunicaciones tácticas, lo que depende de las distancias entre el *jammer* y el blanco y el uso de las técnicas de protección electrónica que el blanco pueda hacer. Las consideraciones a tener presente para el *jamming* de sistemas de comunicaciones tácticas son presentadas en la Tabla 4.1. La efectividad del *jamming* contra los sistemas de comunicaciones tácticas tiene una dependencia directa de las capacidades y la información generada por los sistemas de apoyo electrónico.

SUBSISTEMAS DE COMUNICACIONES TÁCTICAS	VULNERABILIDADES	PROTECCIÓN
Troncales	Antenas altas	Antenas direccionales, larga distancia entre el receptor y el *jammer*
CNR *(Combat Network Radios)*	Antenas omnidireccionales, distancias cortas	Salto de frecuencia
Distribución de data táctica	Antenas omnidireccionales, distancias cortas entre el receptor y el *jammer*	Fuerte empleo de protección electrónica, incluyendo *spread spectrum*
Aerotransportado	Los receptores de los *up-links* están expuestos	Los receptores de los *down-links* pueden ser protegidos de los *jammers* en tierra

Tabla 4.1: *Jamming* de sistemas de comunicaciones tácticas, vulnerabilidades y medidas de protección [1].

Sistema Troncal Táctico

Interferir los subsistemas troncales es más difícil que interferir los subsistemas de las redes de combate, porque los elementos de las

redes troncales no son desplegados tan cerca de las líneas de fuego, como los subsistemas de redes de combate. El empleo de antenas direccionales en una red de repetidores terrestre hace difícil alcanzar una razón J/S suficientemente alta como para que el *jamming* sea efectivo. Al usar la altitud para superar las limitaciones del terreno, un *jammer* aerotransportado que se encuentra en el eje del radio-enlace de un repetidor terrestre puede interferir las comunicaciones en una dirección, sin embargo, es difícil que un *jammer* aerotransportado pueda encontrar una ubicación en el espacio desde donde pueda interferir ambas direcciones de un radio-enlace repetidor terrestre del tipo dúplex, ya que la única posibilidad será localizarse directamente entre las dos antenas. El alto grado de interconectividad que tienen las redes de repetidores terrestres, hacen que jammear un nodo tenga solo un pequeño impacto sobre la red, a no ser que aquel nodo sea un punto neurálgico de alta convergencia y a su vez muy sensible para la red víctima.

Jamming de Enlaces Satelitales

Los enlaces troncales satelitales pueden ser interferidos usando capacidades tácticas. En el caso de los enlaces satelitales, como cualquier otro tipo de *jamming*, es necesario interferir el receptor, no el transmisor. Esta aclaración se hace presente debido a que los radares tienen sus transmisores y receptores colocalizados. Las comunicaciones satelitales, por otro lado están en el otro extremo, ya que sus transmisores y receptores están muy lejos unos de los otros. Como la mayoría de enlaces satelitales son bidireccionales, la localización del transmisor puede indicar la localización del receptor (que no emite). Esto es importante debido a que las distancias involucradas hacen imperativo contar con antenas direccionales de *jamming* en la mayoría de los casos. Paralelamente, las señales de enlaces satelitales casi siempre utilizan modulaciones digitales, así es que lo discutido en este ensayo acerca del *jamming* digital es totalmente aplicable para este caso.

La Figura 4.1 muestra la geometría del *jamming* de enlaces satelitales. Entonces se puede interferir el receptor del tramo de subida de la señal *(up-link),* que se encuentra en el satélite o el receptor del tramo de bajada de la señal *(down-link),* que se encuentra en la estación terrena. Al tomar el *down-link* se tiene una estación terrena que en

la mayoría de los casos tiene una antena direccional, por lo que se requiere estar muy cerca de la estación terrena o tener suficiente potencia de *jamming* para alcanzar una razón J/S adecuada a través de los lóbulos laterales de la antena, que son de muy baja intensidad. La potencia del *jamming* en el receptor, debe ser lo suficientemente alta como para generar suficientes bits erróneos. Si el *jammer* tiene que estar lejos de la estación terrena, este requerirá mayor potencia de salida. Normalmente, el enlace puede tener cierto nivel de modulación del tipo spread spectrum como protección *anti-jamming* y puede también tener un sistema de corrección de bits erróneos. Estas dos características incrementan la cantidad de potencia requerida para crear una taza de bits erróneos adecuada para que el *jamming* sea efectivo. Ahora, el factor que facilita el *jamming* de este tipo de enlaces es que las señales de los satélites a su llegada a la superficie terrestre generalmente son de bajo nivel de intensidad, debido a las pérdidas de propagación.

Existen dos casos importantes que tiene consideraciones diferentes, esto son el *jamming* de teléfonos satelitales y el *jamming* de GPS *(Global Position System).* Por razones de portabilidad, los teléfonos satelitales tienen antenas del tipo omnidireccionales. Las antenas de haz angosto no son aplicables a estos sistemas porque requieren ser orientadas hacia el satélite. Debido a las pérdidas de propagación de los satélites síncronos, los teléfonos satelitales deben operar con satélites de órbita baja, haciendo que el seguimiento de los satélites sea impracticable. Esto significa que el *jammer* puede ver la misma ganancia de antena que aquella en el teléfono hacia el satélite. Sin embargo, el *jammer* puede usar una antena direccional para optimizar su potencia hacia la localización del receptor (teléfono). Es por esta razón que la protección *anti-jamming* del tipo *spread spectrum* y corrector de bits erróneos, son las únicas medidas de protección *anti-jamming* para teléfonos satelitales.

El GPS, por otro lado, no es un sistema de comunicaciones satelital propiamente tal, sino que un sistema *broadcasting satelital,* pero es un caso importante a considerar para la GE. La señal de GPS recibida en la superficie terrestre es muy débil (del orden de -150 dBm), por lo tanto si el *jammer* puede estar en línea vista con el GPS, solo se debe generar la señal de *jamming* adecuada. Así quedó demostrado en la tesis práctica de titulación de un oficial que egresó de la ACAPOMIL

hace un par de años, mediante la cual se pudo demostrar la debilidad de este tipo de señal ante un *jammer* de baja potencia cuyo costo en componentes no superó los quince mil pesos.

La señal GPS tiene dos niveles de *spread spectrum,* una es pública y disponible llamada "CA code" y otra de acceso altamente restringido llamada "P code". Las señales del tipo CA code tienen cerca de 40 dB de protección *anti-jamming* utilizando códigos abiertos, que aun así permiten ser jammeadas con señales relativamente débiles, bajo condiciones de línea vista.

Las señales del tipo P code tienen un nivel adicional de *spread spectrum* y usan códigos seguros, así es que tienen una protección *anti-jamming* adicional de 40 dB. Por tal razón, una señal de *jamming* debe tener suficiente potencia para superar 80 dB de protección *anti-jamming* y así lograr la razón J/S adecuada. Entonces, como el sincronismo de los equipos de comunicaciones de algunos sistema de mando y control (en todos sus niveles), cuentan con una lectura de tiempo extraída desde la señal de sus GPS (normalmente incorporados en los equipos), se asume que la señal GPS con que operan esos equipos es del tipo P code.

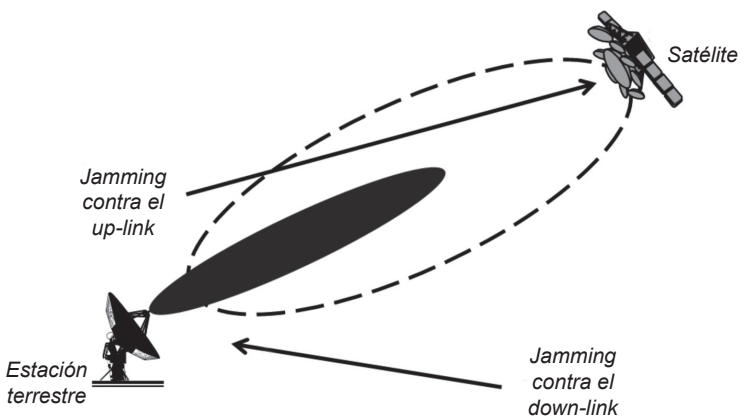

Figura 4.1: El *jamming* de comunicaciones satelitales depende fuertemente de la geometría del escenario para el *jamming,* [9].

Interferir el enlace de subida de un enlace satelital es geométricamente menos difícil que *jammear* el enlace de bajada. Esto debido a

que la antena del receptor en el satélite se encuentra apuntando a la tierra. Para un satélite síncrono con una antena que cubre gran parte de la superficie terrestre, el *jammer* puede estar en cualquier lugar dentro de un 45% de la superficie terrestre y aun así interferir el lóbulo principal. Incluso antenas de ángulo angosto cubren una superficie lo bastante grande desde satélites síncronos o de órbita baja, por lo tanto solo las técnicas *spread spectrum* y de corrección de bits erróneos son medidas de protección electrónica confiables. Incluso, si el enlace de bajada usa una antena de haz angosto y si el *jammer* no puede estar dentro del *footprint* de la antena (zona de la superficie terrestre irradiada por el haz de antena), el *jammer* debe superar el aislamiento de los lóbulos laterales además de las características *anti-jamming* del enlace de subida. En todo caso se debe tener presente que hay un gran inconveniente de pérdidas de propagación a tener presente y que debe ser superado para interferir el enlace de subida, debido principalmente a la distancia en que se encuentra el satélite. La ERP del *jammer* debe ser mayor que la potencia del transmisor de la estación terrena en la cantidad requerida por la razón J/S, el factor de protección *anti-jamming* y el aislamiento de la antena si corresponde.

Subsistemas de Redes de Radios de Combate (CNR)

Una alta proporción de los equipos de *jamming* tácticos se enfoca en los subsistemas de las redes de radio de combate (CNR), debido a su empleo en la cercanía de la línea de fuego del campo de batalla y su empleo de antenas omnidireccionales. El *jamming* de CNR puede atacar a todas las estaciones de una red, a las estaciones de un área en particular o una sola estación si se requiere. Puede ser utilizado para negar comunicaciones o simplemente para forzar a una red encriptada a operar en un modo inseguro, de tal forma que un sistema de apoyo electrónico amigo pueda obtener información de esta. El *jamming* de CNR puede resultar difícil debido al uso de técnicas de protección electrónica, especialmente el salto de frecuencia (FH).

El empleo de *jammers* en vehículos terrestres, le da una movilidad limitada en el campo de batalla. Un vehículo que transporta sistemas de *jamming* debe tener la misma movilidad o superior que la fuerza a la cual está apoyando, por ejemplo, un *jammer* que apoya una formación mecanizada normalmente estará montado sobre un vehículo

blindado. Como para todo transmisor basado en tierra, el rango útil de un *jammer* también basado en tierra está limitado por el terreno, especialmente a partir del VHF y las frecuencias superiores. En algunas circunstancias, esta limitación puede ser utilizada como una ventaja, como cuando un receptor de una red es atacado y se utiliza el apantallamiento del terreno para asegurar que el resto de la red no se percate de los efectos del *jammer*.

Algunos sistemas permiten jammear mientras el vehículo está en movimiento, otros requieren que el vehículo esté detenido y despliegue un mástil. Las ventajas obtenidas por el empleo de un mástil son una reducción en las pérdidas de propagación debido a la mayor altura de la antena y el consecuente aumento del rango de alcance.

Un *jammer* de comunicaciones típico es capaz de interferir al menos una banda militar, por ejemplo, la banda HF desde los 2 hasta los 30 MHz, o la banda VHF que va desde los 30 hasta los 300 MHz. Los sistemas actuales son capaces de interferir bandas mucho más amplias, tanto así que cubren desde los 100 KHz hasta 1 GHz. El *jammer* puede tener la capacidad de transmitir simultáneamente sobre un número determinado de canales, haciendo posible jammear varios blancos a un mismo tiempo. La potencia de salida máxima total de un *jammer* transportado por un vehículo es típicamente superior a 1kW y puede llegar a los 10 kW. Un *jammer* montado en un vehículo es capaz de operar con baterías o con el apoyo de un generador externo. Las baterías son cargadas, siempre y cuando el motor del vehículo permanezca encendido o el generador le entregue la alimentación correspondiente.

El *jammer* puede tener incorporado un receptor del tipo apoyo electrónico, para proporcionar información en la misma forma en que un observador adelantado la entregaría para la artillería. Este receptor opera sobre el rango de frecuencias del transmisor del *jammer* y puede ser un receptor de banda angosta o de banda ancha. Si el *jammer* es capaz de ejecutar *look-through,* el receptor de apoyo electrónico incorporado podrá determinar el estatus de las transmisiones adversarias durante ese tiempo.

Los *jammers* portables y de poco peso, pueden ser transportados por soldados a pie, incluyendo las fuerzas especiales. Estos *jammers* usualmente sacrifican potencia de transmisión por peso y por eso son

diseñados para ser operados en las cercanías del receptor víctima. Naturalmente este tipo de *jammers* opera con antenas de baja altura, que incrementan considerablemente las pérdidas entre el *jammer* y el receptor y también reducen su aplicabilidad en una configuración táctica del tipo *stand-off*. El peso y tamaño de un mástil impide su empleo y transporte por parte de un *jammer* hombre-portado y para superar este tipo de inconvenientes se hace uso de árboles y todo tipo de características naturales del medio en el que se desarrolle el campo de batalla, para proporcionar elevación adicional para las antenas cuando la situación táctica lo permite.

Un *jammer* de comunicaciones hombre-portado moderno cubre porciones similares del espectro electromagnético que un *jammer* transportado en vehículo, también es capaz de transmitir simultáneamente en varios canales. La potencia total de salida del *jammer* hombre-portado puede ser de hasta 20 W o 100 W, usando aplicaciones de amplificación. El peso total de este tipo de sistemas es de alrededor de 10 o 15 kg y el tiempo de operación con sus baterías internas es de algunas horas. También puede contener un receptor de apoyo electrónico de banda angosta. En la siguiente figura se puede apreciar las dimensiones de un equipo *jammer man-pack*. Las inspecciones de seguridad a localidades en Afganistán e Irak por parte de las fuerzas de paz han empleado estos equipos para contrarrestar los efectos de bombas activadas por radiofrecuencia, como es el caso de explosivos activados por señales de telefonía celular.

Figura 4.2: Silueta de un infante con *jammer manpack* (hombre-portado).

Los *jammers* aerotransportados pueden ser desplegados en UAV, helicópteros o aeronaves de ala fija. Mucho cuidado debe ponerse en la instalación de *jammers* de alta potencia en aeronaves para asegurar que no interfieran con la operación de los equipos de navegación. La mayor ventaja que tienen estos *jammers* la obtienen de la elevación de la plataforma que los transporta, superando las limitaciones del terreno que reducen el desempeño de los *jammers* que operan en tierra, pero al mismo tiempo estos pierden la flexibilidad de usar el terreno para interferir un receptor específico mientras dejan sin interferir el resto de los receptores de la red.

Un *jammer* aerotransportado moderno en una aeronave de ala fija tiene la capacidad de cubrir el espectro desde la parte baja correspondiente a la banda HF hasta los 2 GHz y puede ser capaz de atacar emisiones de comunicaciones y no comunicaciones. Su potencia de salida es muy probable que alcance 1 kW. Estos *jammers* obtienen su potencia desde la aeronave y serán capaces de operar mientras la aeronave que los transporta se mantenga en vuelo, interfiriendo múltiples canales simultáneamente. Un ejemplo histórico de *jammer* aerotransportado de grandes prestaciones es el caso del Prowler EA6B, aeronave de la USNAVY presente en cada portaviones. Hoy esta aeronave está migrando al Growler que utiliza como plataforma un F18.

Los *jammers* a bordo de UAV tácticos pequeños tienen propiedades similares a las de un *jammer* hombro-portado. Su capacidad se ve considerablemente aumentada por su mayor altitud de operación. Este tipo de *jammers*, a diferencia de los aerotransportados por aeronaves mayores, toma su energía desde baterías, liberando a su transportador de esa tarea. Los *jammers* transportados por otro tipo de aeronaves tienen capacidades intermedias, siendo la mayor limitación en aviones pequeños el peso que limita la potencia de salida del *jammer*. Paralelamente, las plataformas aéreas pueden contener capacidades de ataque y apoyo electrónico, facilitando la coordinación entre las subdivisiones de la GE.

Por otro lado, los receptores aerotransportados son más propensos a ser vulnerables al *jamming*, debido precisamente a su localización en altura. Esta vulnerabilidad se ve aumentada con el uso de antenas omnidireccionales, incluso para los enlaces que usan antenas direccionales en los terminales terrestres.

Por lo expuesto hasta este punto, para conducir un ataque electrónico se requiere un mínimo de un transmisor. Sin embrago, para sistemas terrestres se requiere al menos dos transmisores, ya que las operaciones en movimiento no siempre lo permiten debido a la combinación de características físicas del terreno y las antenas. Para sistemas aerotransportados, se requiere un mínimo de tres plataformas para permitir el reabastecimiento y mantenimiento, incluso si se dispone de reabastecimiento en vuelo, es poco probable que un sistema de ataque electrónico pueda operar durante el carguío de combustible. Al entregar cobertura, se requiere una operación simultánea de al menos dos plataformas de ataque electrónico aerotransportadas o de superficie, para frecuencias VHF y superiores, aunque esto dependerá del terreno en el que los sistemas se encuentren operando. La cobertura adecuada se puede lograr por medio de la asignación de capacidades de *jamming* al nivel operativo que se encuentre en el campo de batalla. Esta asignación consiste de un mínimo de dos *jammers* basados en tierra o tres plataformas de *jammer* aerotransportados. La capacidad requerida será superior a un canal, lo que se puede lograr asignando *jammers* del tipo multicanal o equipamiento *jammer* extra.

Este análisis sugiere que un mínimo de tres *jammers* aerotransportados o dos *jammers* basados en tierra se requieren en el nivel operativo, cantidad que se incrementa a cuatro o tres respectivamente si se requiere redundancia. Sin embargo, en el campo de batalla moderno, una mayor cantidad de *jammers* siempre podrán ser utilizados y el número asignado a fuerzas de superficie, es el resultado del compromiso de proveer una estructura de fuerza adecuada. Cabe hacer presente que esta capacidad se refiere a plataformas dedicadas exclusivamente a *jamming* capaces de generar un ataque electrónico bajo condiciones *stand-off*, por lo que las capacidades de autoprotección de los *jammers* a bordo de plataformas de ataque no están siendo consideradas en este análisis.

Finalmente, el ataque electrónico debe contar con el apoyo electrónico, para recibir un flujo de información básico. Este apoyo puede ser integrado a los sistemas de ataque electrónico o puede ser provisto por equipamiento separado. El empleo de capacidades de apoyo electrónico separadas, reduce el número de capacidades de apoyo electrónico disponibles para otras tareas y reduce la flexibi-

lidad del despliegue del total de las capacidades. Normalmente, se da respuesta con una fuerza compuesta por dispositivos de ataque electrónico que tienen su propia capacidad de *look-through,* la que es aumentada, cuando es posible, por dispositivos de apoyo electrónico. Hasta aquí se asume el empleo del ataque electrónico en operaciones convencionales de alta densidad. Para el caso de operaciones dispersas, se requiere un mayor número de sistemas de ataque electrónico, debido a las limitaciones en rango impuestas por el terreno.

El apoyo electrónico requiere de al menos dos sistemas receptores de búsqueda capaces de operar en movimiento y en caso de requerir redundancia, este número aumentará. La cobertura que entregue en el teatro de operaciones se logrará con sistemas asignados al nivel operativo, siendo un número de tres dispositivos de búsqueda el mínimo requerido. El mismo criterio aplica para interceptar señales, aunque el número de canales que necesariamente tendrán que ser simultáneamente monitoreados puede indicar un mayor requerimiento en número de sistemas de interceptación. Debido a que la cobertura en comunicaciones requiere de sistemas de búsqueda y de sistemas de interceptación, estos deben ser localizados uno al lado del otro, aunque estos sean equipos separados, con el objetivo de que lo que los sistemas de búsqueda detecten, sea entregado para su seguimiento (interceptación) por los otros sistemas.

En el caso de los equipos determinadores del ángulo de arribo de una señal (DF - *Direction Finder*), se requiere un mínimo de dos estaciones o tres para cumplir con criterios de exactitud. En el caso del nivel operativo, se estima suficiente contar con un número de seis unidades y para el caso de plataformas aerotransportadas, este número se puede reducir a cuatro.

Las funciones de búsqueda, interceptación y DF pueden ser integradas a un único receptor que lo más probable es que sea del tipo digital y una de las principales ventajas de esta condición puede ser la velocidad del manejo de los blancos desde la búsqueda hasta la interceptación y DF, que pueden aumentar el apoyo electrónico contra las cada vez más cortas señales, que cambian tan rápidamente en el campo de batalla.

Radio Localización de Emisores

Para ejercer las funciones del mando y control, los puestos estratégicos y operativos deben forzosamente transmitir señales hacia las fuerzas desplegadas, sean estas infantes, vehículos de superficie, aeronaves u otro tipo de unidades, y estos de igual forma requieren transmitir señales para reportarse o simplemente entregar información útil a los puestos de mando, ejecutando su misión y cerrar el ciclo de C2. Estas unidades pueden no ser vistas producto de la presencia de niebla o humo, mimetismo, oscuridad o porque se encuentran más allá de la línea de vista del adversario, pero la interceptación de las señales que emiten sus transmisores no solo las delatan, sino que entregan la localización de ellos, que corresponde a la ubicación física de esas fuerzas desplegadas. Un análisis inmediato de las señales transmitidas desde esa ubicación, normalmente identifica el tipo de fuerza desplegada, pudiendo ser esta un sistema de armas, una unidad militar determinada, un buque o una aeronave. De esta forma, la localización e identificación de fuerzas apoya a la conducción de las fuerzas propias, alertando la posibilidad de ataques inminentes, evitando amenazas, seleccionando e implementando el ataque electrónico idóneo, generando información para el orden de batalla electrónico (OEB), entregando información de designación de blancos y afinando la orientación de sensores ópticos de reconocimiento.

Todo lo descrito en los dos últimos párrafos se refiere a la capacidad inherente de la GE y la SIGINT referida a localizar la fuente emisora de las señales adversarias, que usualmente se le conoce como *Direction Finding* (DF). Los sistemas de GE y SIGINT requieren localizar los emisores de señales debido a varias razones, siendo las más recurrentes las enumeradas en la Tabla 4.2. De todas maneras, se debe tener en cuenta que la exactitud de esta información depende del radio efectivo letal de las armas empleadas para atacar los blancos parametrizados por la información de localización y esa exactitud también dependerá de la situación táctica que se viva. Esta información es tabulada y utilizada para crear el OEB, que es un documento con información de detalle, referida al tipo y cantidad de sistemas electrónicos dispuestos por el adversario en contra de las fuerzas propias.

En muchos casos la exactitud de la localización es menos importante que la resolución que se pueda proporcionar. La resolución es el

grado en que un sistema de DF puede determinar el número de diferentes emisores están presentes en su rango de operación. Por lo tanto, un sistema que recolecta información de localización de emisores para el OEB, necesita la suficiente resolución para identificar emisores que se encuentren colocalizados, diferenciarlos, obtener su data y entregar esta información para que sea considerada en el OEB.

OBJETIVO	VALOR	EXACTITUD REQUERIDA
Orden Electrónico de Batalla (EOB)	Localización de tipo de emisores asociados con sistemas de armas específicos y unidades mostrando la fuerza del adversario, despliegue y misión	Media - ≈ 1 km
Localización de sensores de armas (autoprotección)	Permite enfocar la potencia del *jamming* o maniobrar para evitar amenazas	Baja - un ángulo general y un rango ≈ 5 km
Localización de sensores de armas (autoprotección)	Permite evitar amenazas por parte de otros combatientes propios	Media - ≈ 1 km
Localización de instalaciones adversarias	Permite la búsqueda y reconocimiento y el seguimiento de señales por medio de dispositivos del tipo *homming*	Media - 5 km
Localización de blancos de precisión	Permite el ataque directo por bombas inhertes o artillería	alta - ≈ 100 m
Diferenciación de emisores	Permite listar por localización para seperación de amenazas por procesos de identificación	Baja - ángulo general y distancia ≈ 5 km

Tabla 4.2: Implicancias de los objetivos de la localización de emisores [3].

El incremento del empleo de métodos para ocultar señales por medio de la variación de sus parámetros, tales como el salto de frecuencia y la frecuencia aleatoria de repetición de pulsos, ha hecho que la diferenciación de localización de emisores sea una capacidad más importante para los sistemas DF actuales. La enumeración de pulsos o los saltos de señales de comunicaciones, por su localización puede ser la única forma de determinar que ellas son de la misma fuente

y esta puede ser la única forma de recolectar la data necesaria para diferenciar el tipo de amenaza asociada.

La localización de emisores se logra aplicando una o la combinación de algunas de las técnicas que se describen a continuación, en donde los resultados de una técnica pueden ser contrastados con los de otra para corregir u obtener una solución de mayor exactitud.

La primera y más conocida de las técnicas es la triangulación, que localiza a un emisor en la intersección de dos líneas desde dos posiciones distintas en el plano (dos dimensiones), cuando se tiene dos líneas que se interceptan, ambas líneas corresponden al acimut desde dónde la señal es recibida en dos sitios distintos de interceptación, según se puede ver en la Figura 4.3. Cuando el emisor tiene que ser localizado en tres dimensiones, además de medir el acimut desde cada sitio de interceptación, también debe medirse la elevación del arribo de la señal en cada uno de ellos. Será altamente conveniente tener un tercer sitio de interceptación, de tal manera que la localización del emisor sea definida por la intercepción de tres líneas, donde la tercera línea pasa a ser una forma de validación, ya que un error en una línea puede inducir a un gran error de localización, [3].

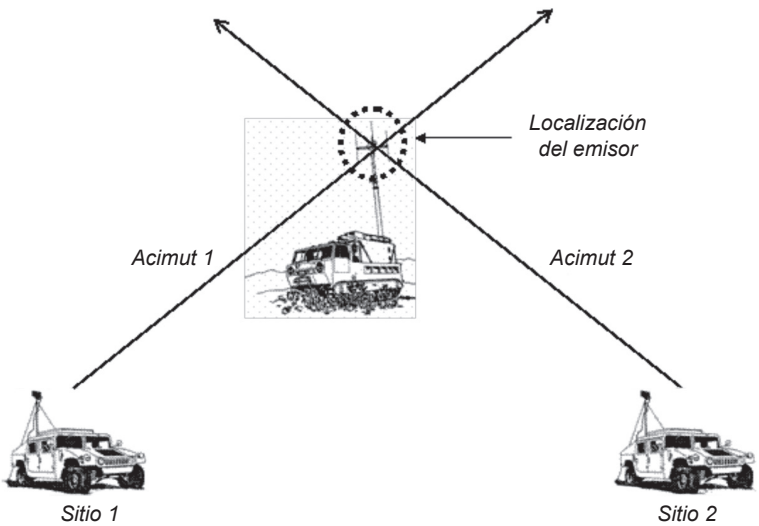

Figura 4.3: La triangulación implica tomar medidas del ángulo de arribo de la señal (acimut), desde más de un sitio, por uno o más sistemas interceptores.
Fuente: elaboración propia.

La segunda técnica corresponde a la medición del ángulo y la distancia desde solo un sitio de interceptación (ver Figura 4.4). La mayoría de los radares localizan los blancos de esta forma, ya que son radiadores activos y miden distancia directamente, pero los sistemas de GE y SIGINT deben medir distancia pasivamente. Los sistemas de localización desde un sitio de interceptación utilizan este principio para determinar distancia, principalmente en las comunicaciones del tipo HF, midiendo el ángulo de elevación de la señal, ya que esta proviene de una reflexión en la ionósfera y de esta forma determinar la distancia al transmisor. Por otro lado, los Radar Warning Receivers (RWR) a bordo de plataformas aéreas, miden la potencia de la señal recibida y determinan la distancia al radar (cuya potencia ya es conocida), calculando el rango al cual las pérdidas de transmisión reducirían su potencia radiada conocida al nivel que se está recibiendo. Esta técnica, tanto para comunicaciones como para señales de radar tiene baja exactitud en la localización de los emisores, [3].

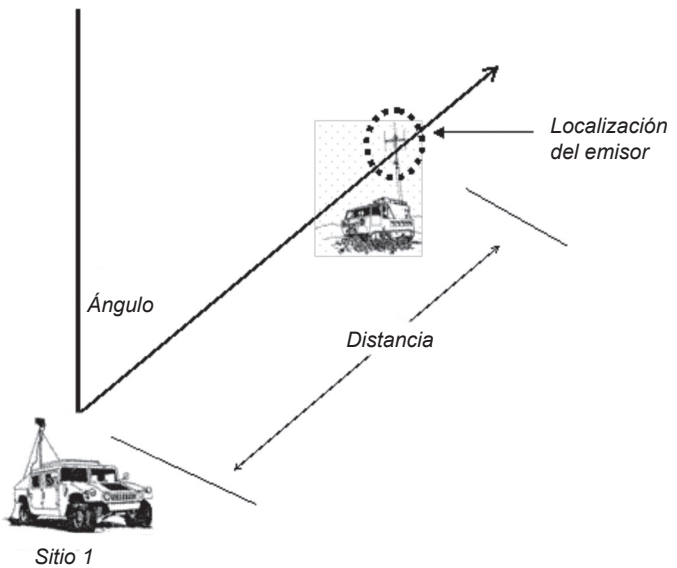

Figura 4.4: Para esta técnica (medición de ángulo y distancia desde solo un sitio de interceptación), la distancia del emisor se deriva de la intensidad de señal recibida en el sistema DF. Fuente: elaboración propia.

Una tercera técnica es la medición de distancias múltiples. Esta técnica localiza al emisor en la intersección de dos arcos de radio conocidos (ver Figura 4.5). Para la GE y la SIGINT existen dos pro-

blemas considerables, primero los arcos desde los dos puntos de interceptación se intersectan en dos puntos, ¿cuál de estos es la localización del emisor?, una segunda técnica debe utilizarse para solucionar esta ambigüedad. El segundo problema es que es muy difícil medir pasivamente y con exactitud la distancia a un transmisor no cooperativo, aquí se emplean sistemas que miden la diferencia del tiempo de arribo de las señales que proporcionan una localización de mayor exactitud utilizando esta técnica con pequeñas variaciones, [3].

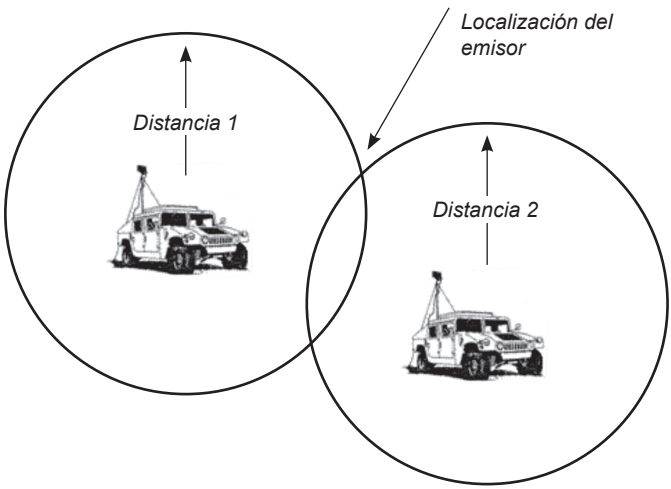

Figura 4.5: Localización del emisor por medición de distancias múltiples, localiza el emisor en la intercepción de dos arcos, pero como la solución es doble, requiere del apoyo de otra técnica para solucionar la ambigüedad. Fuente: elaboración propia.

Una cuarta técnica utilizada por equipos SIGINT aerotransportados, entrega la localización de un emisor por medio de la medición de dos ángulos y la diferencia de elevación entre estos (ver Figura 4.6). Así cuando la diferencia de altitud entre el sistema DF y el transmisor es conocida, la localización del transmisor puede ser determinada por sus ángulos de acimut y elevación. El mejor ejemplo de la aplicación de esta técnica es la localización de emisores basados en tierra desde una aeronave con sistema de navegación inercial, que facilita al computador del sistema de interceptación el manejo de data, que al procesarla puede entregar la elevación del sitio del transmisor en un mapa digital, [3].

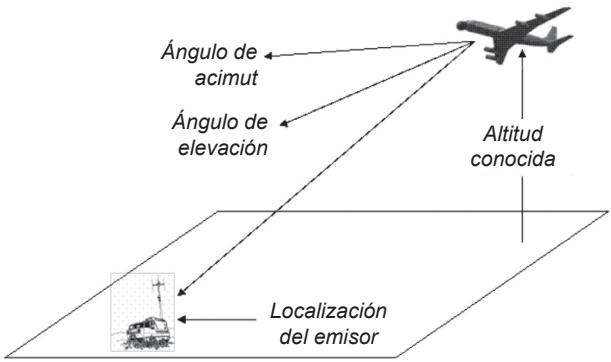

Figura 4.6: Si el sistema conoce la diferencia de altitud entre la aeronave que lo transporta y el emisor, la medición de los ángulos de elevación y acimut determinarán la posición del emisor. Fuente: elaboración propia.

La quinta técnica se basa en la medición de múltiples ángulos desde un sistema de interceptación en movimiento. Un sistema de interceptación puede localizar un transmisor midiendo los ángulos de arribo de la señal desde distintos sitios (ver Figura 4.7). Pero esta técnica requiere grandes períodos de operación y desplazamiento de los sistemas interceptores, ya que las mediciones deben tener cerca de 90° de separación, exigiendo que el interceptor viaje una vez y media aproximadamente la distancia al blanco, para obtener una segunda medición y a su vez que el transmisor permanezca en esa condición y estacionario, lo que es impracticable en la realidad, incluso para sistemas aerotransportados, [3].

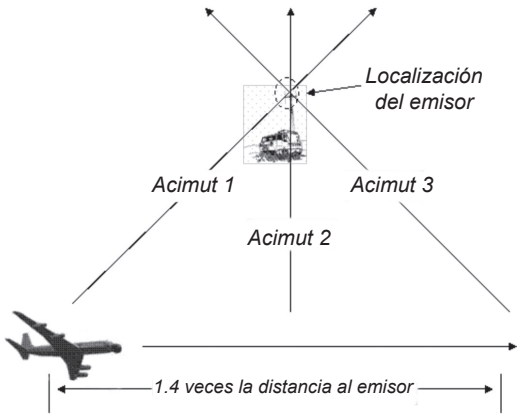

Figura 4.7: Un interceptor en movimiento puede medir la dirección de una señal en distintos momentos, comparar esa información y determinar la localización del transmisor fijo. Fuente: elaboración propia.

Capítulo V
El Nuevo Escenario

Con el desarrollo tecnológico que se experimenta en estos días en que la nanotecnología, la obsolescencia continua de cada procesador antes de que salga a la venta, tal vez antes de que se inicie su producción, las increíbles velocidades de transmisión, el incremento de la conectividad inalámbrica para cada vez una mayor cantidad de dispositivos, no solo de uso civil sino que militar dentro de redes militares obviamente, queda demostrado que así como en lo civil, en el ámbito militar la tecnología va quedando rápidamente obsoleta frente a los nuevos sistemas desarrollados y en proyecto de desarrollo. Un claro ejemplo de esta contingencia es la convergencia al tendiente empleo de productos COTS *(Commercial off the Shelf)*, con el objetivo de ampliar las posibilidades de empleo de hardware y software en futuras actualizaciones *(up-grades)* de sistemas y equipamiento en general, con la clara idea de no verse forzados a renovar completamente sistemas complejos o equipos que por tecnología, mantenimiento y efectividad, ya no son útiles para enfrentarse en la lucha por el control del EEM. Por tecnología el ejemplo es claro, cuando se lucha en bandas de frecuencias sobre las cuales no se dispone de medios para operar en ellas. Por mantenimiento, la exposición a tener que operar sistemas cerrados de fabricantes exclusivos o equipos cuyo software es dependiente de hardware único y no comercial, han hecho padecer al personal de mantenimiento responsable y a las organizaciones logísticas pertinentes. Por efectividad, por ejemplo se tiene los sistemas de comunicaciones protegidas, que lo más sensato es optar por protocolos o estándares internacionales, configurables y basados en algoritmos con llaves y sincronismos definidos por el operador y no a sistemas cerrados que no interactúan con ningún equipo más que del mismo fabricante… en un mundo globalizado en el que una nación tendrá que enfrentar un teatro de operaciones lejano junto a las fuerzas de otra nación (como amigo),

requerirán de estándares o protocolos para poder interoperar en el EEM y los sistemas cerrados aquí no tienen cabida por incompatibilidad natural.

Especial atención debe ponerse en los procesadores de los equipos de GE. La actualidad dicta el empleo de los DRFM *(Digital Radio Frequency Memories),* que son dispositivos capaces de desarrollar tareas inherentes al reconocimiento de emisiones detectadas, su almacenamiento en memoria digital y la generación del ataque correspondiente a velocidades no comerciales actuales. Un *jammer* que integra en su hardware la capacidad de un DRFM digitaliza la señal que recibe a la frecuencia y ancho de banda adecuado para representar la señal, la que no sufre la degradación natural de los sistemas de memoria análogos. De esta forma el DRFM puede modificar la señal de radiofrecuencia antes de retransmitirla pudiendo ajustar convenientemente la RCS aparente del blanco falso, su rango, velocidad y ángulo de aproximación, presentando de esta forma un obstáculo significativo para los radares y sensores de víctimas.

Por otro lado, hablando de sistemas C2 y entendiendo a estos como redes de mando y control desplegadas en un teatro de operaciones, principalmente inalámbricas, hoy se utilizan protocolos de comunicaciones que encontramos en las redes civiles, sin ir más lejos el formato "ip" de internet está presente en un buen porcentaje de las redes de los sistemas C2. En otras palabras, las vulnerabilidades de este protocolo o de las aplicaciones que pueden operar sobre él, hoy afectan por igual a las redes civiles y militares y dentro de las militares incluidas las de sistemas C2. Es decir, el desarrollo de "malwares" (software malicioso), virus informáticos y todo tipo de vulnerabilidades informáticas explotadas y atacadas por los denominados *hackers*, hoy pueden tener víctimas tanto en redes civiles como militares. Cuando esta actividad se desarrolla con capacidades organizadas por un Estado para enfrentar a otro Estado y es conducida ya no por un grupo de *hackers* locales, sino que por un grupo de profesionales dedicados a explotar vulnerabilidades de redes adversarias por medio del ataque coordinado, se le denomina ciberguerra y toma lugar en el ciberespacio. Se entiende el ciberespacio como toda red de computadores que transmiten data digital de voz, videos o archivos, siendo estas redes físicas o inalámbricas, de formato ip o de cualquier otro protocolo, pudiendo por ejemplo ser redes telefó-

nicas, de televisión, de radiotransmisión, la misma internet, pero no exclusivamente, y otras más.

Pero, ¿qué tiene que ver la ciberguerra con la GE?

Primero, la comunidad de GE a nivel mundial y no distintamente en Chile, es una comunidad pequeña y altamente tecnológica, que se ha desarrollado con la integración de sistemas existentes y en proyecto, valiéndose de la experiencia que la evaluación de las capacidades de esos sistemas les entrega para formar el conocimiento de la lucha por el dominio del EEM. Estos combatientes se encuentran en la planificación, ejecución y control de toda operación que involucre el despliegue de fuerzas que hacen empleo del EEM para ejecutar su misión, es decir, desde las comunicaciones que puedan utilizar la infantería, hasta los designadores láser que puedan portar aviones de combate, o los sensores de búsqueda (radar, IR y otros) que puedan utilizar los buques y los sistemas de armas asociados a estos. Desafortunadamente ellos luchan con frecuencia por un reconocimiento a la importancia de esta actividad. Se debe tener presente que la GE lucha dentro del EEM y para tener su control este tipo de lucha es espectral, no visible, no siempre figura en los *diebriefings* de las misiones ni en los *mass diebrifing* de ejercicios a nivel operativo, naturalmente por la complejidad y reducido número de especialistas que la dominan.

Por otro lado, el ciberespacio no puede existir sin el libre empleo del EEM, medio natural de la propagación de su data y naturalmente los problemas de ciberseguridad son más factibles de ser experimentados por un ciudadano normal, cosa que vemos a diario en vulneraciones a las redes civiles o el simple robo de información desde bases de datos residentes en redes supuestamente protegidas, como es el caso de los fraudes bancarios que han afectado a un número considerable de ciudadanos a través de la violación de sus cuentas bancarias y tarjetas de crédito. Así la ciberguerra se hace más notoria porque tiene cobertura civil y mediática (por ejemplo, el colectivo Anonymous, el caso wikileaks y otros), que expone esta actividad a los noticieros y los medios en general, con la consecuente realidad de los ataques registrados a nivel internacional también. Respecto a esto último es que se debe tener presente lo ocurrido en Estonia el año 2007, ocasión en que por una decisión política que afectó a la comunidad Rusa residente, Estonia enfrentó una parálisis casi total de una parte

altamente sensible de su infraestructura crítica, debido a un ciberataque masivo que bloqueó todas las páginas web del gobierno (se debe imaginar el registro civil e impuestos internos fuera de servicio, justo los días de declaración de renta), también todos los medios de comunicación quedaron desconectados imposibilitándoles informar lo que ocurría, bloqueo total del servicio bancario vía web e inutilización total de la red de cajeros automáticos y finalmente un ataque sistemático a los sitios web de las universidades más importantes, todo esto duró poco más de un mes.

Entonces, el acelerado desarrollo tecnológico global incluye tecnologías COTS, sistemas definidos por software, tecnologías en red y el repunte exponencial del desarrollo de la tecnología de circuitos integrados, los que en su conjunto están impactando fuertemente el entorno de amenazas tanto para la GE como para ciberseguridad y el tipo de soluciones que se pueden desarrollar contra esas amenazas. Paralelamente, se debe observar la homogenización de la tecnología que busca la compatibilidad de los sistemas en su interconectividad y formatos de soporte de información. Por esto, tanto la GE y la ciberseguridad se enfrentarán a un panorama de amenazas variables, diversas y de rápida ocurrencia y evolución. Hoy, los sistemas modernos ya son vulnerables a los ciberataques, porque tecnológicamente estos son predominantemente definidos por software y del tipo COTS, con lo que las posibilidades de ataques también se incrementarán.

Entonces, en el campo de batalla digital existe ahora una relación que obligará a la coordinación de las operaciones de GE con las llevadas a cabo por la ciberguerra, cuando al menos estas se lleven a cabo en contra de sistemas C2, sin perder de vista que ambas son ejecutadas para lograr la superioridad en el gran paraguas de la Guerra de la Información.

Finalmente, la guerra no se ganará simplemente por tener una ventaja tecnológica, sino por cómo se integra y utiliza la tecnología.

REFERENCIAS

1 FRATER, Michael R.; RYAN, Michael; *Electronic Warfare for the Digitized Battlefield;* Artech House, 2001.

2 *US Army Field Manual FM 100-6; Information Operations;* 1996.

3 ADAMY, D. *Electronic Warfare 102;* Artech House, 2004.

4 SKOLNIK, M. *Introduction to Radar System,* 3rd Edition, Mc Graw Hill, New York, 2001.

5 USAF, *Electronic Warfare Fundamentals,* November, 2000, 4349 Duffer, Drive, Ste. 437, Nellis AFB NV 89191-7007.

6 ADAMY, D. *Electronic Warfare 101;* Artech House, 2001.

7 PACE, P.; JARPA, P. and others; *Low Probability of Intercept Radar;* Artech House, 2004.

8 POISEL, R. I*ntroduction to Communication Electronic Warfare Systems;* Artech House, 2002.

9 ADAMY, D. *Advanced Electronic Warfare* (Class Notes); AOC Course, 2007.

10 SCHLEHER, C. *Electronic Warfare in the Information Age;* Artech House, 1999.

11 ADAMY, D. *Electronic Warfare 103;* Artech House, 2009.