MARINHA DO BRASIL

DIRETORIA DE ENSINO DA MARINHA

CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM

GUERRA ELETRÔNICA

1ºTen (QC-CA) PAULO CÉSAR RIBEIRO MARCIANO

MEDIDAS DE ATAQUE ELETRÔNICO E PERSPECTIVAS PARA A MARINHA DO BRASIL

Rio de Janeiro

2018

1ºTen (QC-CA) PAULO CÉSAR RIBEIRO MARCIANO

MEDIDAS DE ATAQUE ELETRÔNICO E PERSPECTIVAS PARA A MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Guerra Eletrônica

Orientadores:

CC Alessandro Roberto dos Santos, MSc

Fernando da Rocha Pantoja, PhD

CIAW

Rio de Janeiro

2018

1ºTen (QC-CA) PAULO CÉSAR RIBEIRO MARCIANO

MEDIDAS DE ATAQUE ELETRÔNICO E PERSPECTIVAS PARA A MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Guerra Eletrônica.

Aprovada em_____ _____

Banca Examinadora:

Fernando da Rocha Pantoja, PhD - CIAW _____

CC Alessandro Roberto dos Santos, MSc - CGEM _____

Gian Karlo Huback Macedo de Almeida, MSc - CIAW _____

CIAW

Rio de Janeiro

2018

Dedico este trabalho a todos aqueles que contribuíram para a sua realização e a todos os alunos do curso de Aperfeiçoamento Avançado em Guerra Eletrônica

AGRADECIMENTOS

Agradeço ao Centro de Instrução Almirante Wandenkolk por todo apoio prestado no decorrer do curso de Aperfeiçoamento Avançado em Guerra Eletrônica (C-ApA-GE). Aos meus orientadores, pelos ensinamentos que em muito contribuíram no desenvolvimento do trabalho e também pelo tempo despendido no decorrer do curso. A todos os professores do C-ApA-GE pelos ensinamentos, demonstrações e momentos de inspiração.

A vida vai ficando cada vez mais dura perto do topo

Friedrich Nietzsche

MEDIDAS DE ATAQUE ELETRÔNICO E PERSPECTIVAS PARA A MARINHA DO BRASIL

Resumo

A superioridade aérea na guerra moderna é considerada uma das chaves para o sucesso em conflitos que ocorrem pelo mundo. Sendo assim, uma aeronave de combate deve ter um alto grau de sobrevivência em ambientes cercados de tecnologias avançadas de combate. Neste contexto a Guerra Eletrônica (GE) tornou-se um recurso vital em todas as fases das operações aéreas modernas e é capaz de desempenhar um papel fundamental nos níveis tático, operacional e estratégico das operações aéreas. Dentro do universo da GE destacam-se as Medidas de Ataque Eletrônico (MAE). As MAE têm como objetivo evitar que o inimigo use seus sistemas de armas de forma eficaz, buscando não utilizar as armas convencionais e são ações tomadas para evitar ou reduzir o uso efetivo, por parte do oponente, do espectro eletromagnético e também degradar, neutralizar ou destruir sua capacidade de combate por meio de equipamentos e armamentos que utilizem este espectro. O presente trabalho realiza uma abordagem sobre os tipos de MAE, descreve as técnicas mais comuns utilizadas para realizar Bloqueio e Despistamento na GE e comenta tecnologias como as Armas de Energia Direcionada e Mísseis Anti-Radiação. Algumas seções são dedicadas para descrever as principais táticas empregas por aeronaves em missões de GE, bem como dispositivos que essas aeronaves utilizam durante as MAE. Os dois últimos capítulos abordam aeronaves utilizadas nas missões de ataque eletrônico, sendo um deles destinado a detalhes dos equipamentos de ataque eletrônico embarcados e o outro aborda o emprego tático das aeronaves de MAE. O trabalho expõe que as Forças Armadas mais desenvolvidas atualmente possuem grande domínio de tecnologias usadas nas MAE. Países como os Estados Unidos investem maciçamente em pesquisas e desenvolvimento de armamentos de GE de forma a se aperfeiçoarem cada vez mais e tentando ao máximo seguir as evoluções em dispositivos eletrônicos, materiais elétricos e sistemas de processamento digital. Ficou clara a importância de todas essas tecnologias na guerra moderna, deixando a Marinha do Brasil ciente do nível atual da GE em aeronaves.

Palavras- chave: Guerra eletrônica, medidas de ataque eletrônico, aeronaves de ataque eletrônico, dispositivos de ataque eletrônico, técnicas e táticas de MAE.

LISTA DE FIGURAS

LISTAS DE SIGLAS E ABREVIATURAS

GE	Guerra Eletrônica
EEM	Espectro Eletromagnético
AçGE	Ações de Guerra Eletrônica
CGE	Capacidade de Guerra Eletrônica
AGE	Atividades de Guerra Eletrônica
MAGE	Medidas de Apoio à GE
MAE	Medidas de Ataque Eletrônico
MPE	Medidas de Proteção Eletrônica
IADS	Integrated Air Defense Systems
MAP	Microondas De Alta Potência
NGJ	Next Generation Jammer
USAF	United States Air Force
SPJ	Self-Protection Jamming
SOJ	Standoff Jamming
EJ	Escort Jamming
RGPO	Range Gate Pull Off
RGPI	Range Gate Pull-In

SUMÁRIO

1. INTRODUÇÃO

A Marinha do Brasil aborda na sua Doutrina Militar Naval (DMN) alguns conceitos importantes de GE. Conforme a DMN a defesa aeroespacial ativa abrange os interceptadores, os mísseis, a artilharia e as Medidas de Ataque Eletrônico (MAE). A defesa aeroespacial passiva compreende a camuflagem, a dispersão, as manobras evasivas e o emprego das Medidas de Apoio à Guerra Eletrônica (MAGE) e das Medidas de Proteção Eletrônica (MPE).

As Medidas de Guerra Eletrônica (MGE) abrangem as ações efetivamente realizadas no decorrer de uma operação de guerra naval. Sua natureza é fundamentalmente tática e seu emprego deve estar amparado por um planejamento e pela adequabilidade dos procedimentos e equipamentos utilizados. As MGE são divididas em três ramos: Medidas de Apoio à Guerra Eletrônica (MAGE), Medidas de Ataque Eletrônico (MAE) e Medidas de Proteção Eletrônica (MPE), conforme o conjunto de ações tomadas para (EMA 305, 2017):

- MAGE: monitoração, busca de interceptação, localização, análise, avaliação e correlação e registro dos sinais eletromagnéticos irradiados pelo opositor, com a finalidade de explorá-las em apoio às operações.
- MAE: impedimento ou redução do uso efetivo, por parte do inimigo, do espectro eletromagnético e, também, degradação, neutralização ou destruição de sua capacidade de combate por meio de equipamentos e armamentos que utilizem este espectro. As MAE podem ser subdivididas em não destrutivas e destrutivas.
- MPE: proteção de meios, sistemas, equipamentos, pessoal e instalações, a fim de assegurar o uso efetivo do espectro eletromagnético, a despeito do emprego de MAE por forças amigas e inimigas.

As MAE empregadas por aeronaves serão o foco do trabalho, as subseções abaixo descrevem alguns detalhes dessa abordagem.

1.1 Apresentação do Problema

A Guerra Eletrônica (GE) visa manter a liberdade de ação no espectro eletromagnético para forças amigas, ampliar e certificar a capacidade de emprego eficiente das emissões eletromagnéticas próprias e negar, impedir, dificultar ou tirar proveito das emissões inimigas. Nesse contexto, buscam-se situações como:

- Obter dados do oponente, a partir das emissões eletromagnéticas de interesse utilizadas pelo oponente;
- Impedir ou dificultar o uso do espectro eletromagnético pelo oponente, pelo uso da irradiação, reirradiação, reflexão, alteração ou absorção intencional de energia eletromagnética, e;
- Assegurar a utilização eficaz e segura das próprias emissões eletromagnéticas, a despeito das ações de GE empreendidas pelo oponente ou formas de interferências não-intencionais.

No atual cenário a GE deve criar efeitos no espectro eletromagnético que possam suportar as forças amigas gerando controle, detecção, negação, interrupção, degradação, proteção, destruição. Planejar uma operação militar sem o acesso ao espectro eletromagnético pode resultar em uma ação totalmente ineficaz. Neste contexto a GE tornou-se um recurso vital em todas as fases das operações aéreas modernas e é capaz de desempenhar um papel fundamental nos níveis tático, operacional e estratégico das operações aéreas. Assim, uma Força Aeronaval pode criar as condições mais favoráveis antes de um ataque, assim como executar o ataque já em combate. Dentro da GE encontram-se as Medidas de Ataque Eletrônico, elas envolvem ações tomadas para prevenir ou reduzir o uso do espectro eletromagnético ao inimigo e tem papel crucial nesse novo modelo de guerra aérea.

O estudo em questão pretende abordar temas relacionados à GE em aeronaves e tem um foco nas MAE clássicas e as empregadas atualmente.

1.2 Justificativa e Relevância

O desenvolvimento de avançados sistemas de defesa aérea pelo mundo compromete cada vez mais o sigilo de aeronaves que operam no espaço aéreo, sendo necessário o apoio contínuo da Guerra Eletrônica em um combate entre diferentes Forças. Os sistemas de armas e as tecnologias da guerra estão em constante evolução e se modificando de forma cada vez mais rápida.

Na atual conjuntura mundial os avanços de ameaças emergentes estão atenuando a eficácia de algumas tecnologias empregadas em missões de GE. Um dos exemplos desses avanços é sentido pela tecnologia *stealth.* Essa tecnologia consiste basicamente em plataformas (normalmente aeronaves) mais difíceis de serem detectadas por radares, sendo conhecida a mais de quarenta anos. Os sistemas de defesa aéreos cada vez mais robustos estão se proliferando em todo o mundo. Os IADS (Sistemas de Defesa Aérea Integrados) estão altamente capacitados. As IADS estão sendo construídos baseados em aeronaves de combate modernas, possuem radares avançados de múltiplas frequências para aquisição de alvos e controle para ataque. Além disso, os mísseis superfície-ar (SAMs) encontra-se altamente precisos e com alcance cada vez maior. Os SAMs desenvolveram-se tão rapidamente que superaram as vantagens da aeronave *stealth*, projetada para derrotar as IADS anteriores. Esse contexto é o resultado de avanços em sistemas eletrônicos e computacionais que ocorreram muito mais rapidamente do que os avanços na aeronáutica, além disso, esses sistemas eletrônicos envolverem menos custos. Portanto, para combater ameaças IADS cada vez mais capazes, fazem-se necessários novos recursos de ataque eletrônico para garantir que futuras missões aéreas possam ser realizadas com sucesso.

Em países como os Estados Unidos algumas medidas são adotadas pelo seu Departamento de Defesa e elencadas abaixo (BARNO; BENSAHEL; DAVES, 2014):

- Criar um programa doutrinário e de investimentos para ataque/proteção eletrônico (a) indispensáveis para penetrar com sucesso em futuros ambientes de ataque ou negação aéreos, o *A2/AD*.
- Criar integração doutrinária e operacional entre os vários componentes aéreos e nas várias plataformas.

- Priorizar o desenvolvimento do *Next Generation Jammer* (NGJ), que consiste em uma tecnologia nova de sistemas de interferência. Bem como as outras capacidades semelhantes que surgem, e
- Ter uma "política de aquisição" eficiente para que os avanços nos sistemas eletrônicos possam ser rapidamente operacionalizados.

No atual cenário de guerra, as Medidas de Ataque Eletrônico (MAE) são fundamentais também em apoio às operações de defesa para prevenir, deter e derrotar todas as ameaças inimigas, como mísseis, aeronaves, ameaças marítimas e outros sistemas hostis. As situações onde o objetivo é a não detecção da aeronave, ou seja, a sua sobrevivência a missão é de preservação da mesma assim como reduzir a força de ataque. Caso contrário seria necessárias armas de apoio e aeronaves de escolta para combater as modernas defesas aéreas existentes atualmente.

Neste momento observa-se que a utilização de tecnologias de MAE aplicadas às aeronaves da Marinha do Brasil pode representar a preservação de meios da Força Aeronaval de forma a ganhar autonomia em possíveis combates, evitando a necessidade de aquisição de outras armas de combate caso a aeronave não possua nenhum método de defesa perante uma GE.

Portanto, explorar e pesquisar os avanços em GE em ambientes aéreos, envolvendo técnicas e equipamentos empregados por aeronaves, é importante para que a Marinha do Brasil possa tomar consciência do nível tecnológico que os outros países se encontram e assim, buscar desenvolver-se na área.

1.3 Objetivos

As seções seguintes descrevem os objetivos do trabalho feito, dando uma ênfase geral na primeira seção e por fim relata os objetivos específicos na segunda secção.

1.3.1 Objetivo Geral

O domínio da GE significa ter poder de combate contra o inimigo, sendo capaz de interromper ou desativar comunicações, radares, sistemas eletrônicos, baterias e outras atividades importantes das forças inimigas, bem como proteger as forças amigas.

Os efeitos psicológicos sobre as percepções e a moral de um inimigo também podem ser observados como pontos positivos da GE.

Observa-se também, que deter essas tecnologias significa apoiar às operações de defesa de forma a prevenir, detectar, dissuadir e derrotar todas as ameaças inimigas, como mísseis, aeronaves tripuladas e não tripuladas, ameaças terrestres e marítimas, sistemas aéreos hostis e terrorismo interno ou internacional. A importância desses recursos e o nível de ameaças exigem que os sistemas de MAE modernos sejam efetivos, precisos, eficientes e cada vez mais robustos.

Possuir receptores eletrônicos avançados em aeronaves modernas resulta na detecção de emissores inimigos e capacidade de combate de ameaças mais avançadas. Todos os sistemas são capazes de fornecer a consciência eletrônica da situação para auxiliar uma rápida tomada de decisão através da classificação de ameaças e do mapeamento de emissores.

O trabalho pretende mostrar a importância de todas essas tecnologias para a Marinha do Brasil e busca atualizá-la quanto às inovações tecnológicas para que a mesma tome consciência situacional e possa atualizar seus meios no que se refere a operações aéreas que atuam na GE.

1.3.2 Objetivos Específicos

O trabalho em questão busca inicialmente realizar uma pesquisa sobre as atuais aplicações das MAE embarcadas em aeronaves de Forças Armadas dos Estados Unidos, explorando as táticas de MAE em aeronaves, os dispositivos de MAE e as tecnologias clássicas empregadas nesses combates, bem como as tecnologias que estão sendo desenvolvidas por uma das mais modernas Forças Armadas da atualidade. Ciente de que existe uma grande evolução em sistemas eletrônicos, sensores digitais, processamento de sinais, microeletrônica e novas tecnologias, também é explorada a modernização dos itens supracitados para aplicações na GE. Pretende-se descrever as técnicas, táticas e equipamentos empregados por aeronaves que utilizam ataque eletrônico.

2. REFERENCIAL TEÓRICO

Os trabalhos e documentos mais relevantes para o desenvolvimento do tema foram elencados abaixo e descritos de forma sucinta conforme as subseções.

O livro de (NERI, 2006) aborda por meio de vários capítulos os conceitos básicos sobre sistemas de defesa eletrônica como: sensores, sistemas de armas tradicionais e modernos e muitas concepções envolvendo Guerra Eletrônica (GE). Os principais itens deste livro que contribuíram para o trabalho versão sobre as técnicas de bloqueio e despistamento. Além disso, o livro descreve como modernos sistemas eletrônicos de defesa operam e como eles podem ser usados nas operações militares de hoje e de amanhã.

A obra “Fundamentos de Guerra Eletrônica” (USAF, 2000) é um documento criado pelo Departamento de Defesa da Força Aérea americana e que fornece a base para a compreensão dos conceitos básicos de GE. O texto é construído de forma prática e usa uma abordagem para facilitar a compreensão do leitor sobre os assuntos essenciais associados às aplicações de combate da GE.

Outro documento da Força Aérea americana que foi utilizado no trabalho aborda algumas aeronaves de ataque eletrônico dos Estados Unidos (USAF, 2016). As informações deste relatório contribuíram para a construção do capítulo 6 e 7.

O documento da Força Aérea Brasileira (FAB, 2011) referente a Medidas de Ataque Eletrônico realiza uma abordagem da doutrina de MAE usada pela Força. O documento faz um apanhado sobre os conceitos básicos de ataque eletrônico.

O artigo (QUARANTA, 2008) discute a contribuição das aeronaves em operações militares que envolvam GE. O autor deixa claro que a Guerra Eletrônica no meio aéreo forneceu o controle de segmentos chave do espectro eletromagnético para a detecção de forças. O trabalho afirma que a aeronave detentora dessa tecnologia é usada para interferência em comunicações, possui controle de fogo e técnicas eficazes para aumentar a capacidade de sobrevivência de aeronaves em ambientes hostis. O mesmo autor também publicou outro artigo que aborda a complexidade nas operações que demandam a GE no ar e os sistemas de auto proteção (QUARANTA, 2015). Os tópicos discutidos incluem a neutralização de radares e sistemas eletrônicos através da GE. O autor fala sobre sistemas eletrônicos de defesa *Aselsan AS* que oferecem o

sistema de GE e menciona algumas nanotecnologias que permitem a criação de dispositivos eficazes nessas operações militares.

O artigo de (WILSON, 2017) informa sobre os avanços tecnológicos feitos no campo da guerra eletrônica e os temas discutidos incluem inovações feitas em armas e tecnologias de guerra. Relata os pontos de vista de Gregory Breazile, diretor do setor de Guerra de Informações do Corpo de Fuzileiros Navais dos EUA sobre o tema; e o papel da indústria eletrônica militar na evolução da guerra eletrônica e tecnologias afins, através da pesquisa e desenvolvimento independentes.

O artigo de (KELLER, 2017) informa a escolha da empresa aeroespacial *Lockheed Martin* pelos especialistas em guerra de superfície da Marinha americana (U.S Navy's) e especialistas em defesa de mísseis para desenvolver um sistema de guerra eletrônica de longo alcance baseado em helicópteros aptos a proteger os navios de superfície da Marinha contra as avançadas armas "anti navios" existentes.

Em (QUARANTA, 2015) são abordadas as tecnologias de *microondas de alta potência* (MAP) desenvolvida no Laboratório de Pesquisa, *Kirtland* da Força Aérea americana. A tecnologia está testando uma abordagem inovadora em sistemas aéreos, obtendo resultados notáveis nos campos de antenas, geradores de energia e geradores de microondas. Estes sistemas permitem neutralizar, não apenas perturbar, um sistema eletrônico sem conhecer as frequências operacionais ou outras características de emissão, criando danos permanentes, ao contrário do que acontece com os sistemas de GE tradicionais onde os efeitos terminam uma vez que as operações de bloqueio estão concluídas. Assim como a MAP, outro estudo interessante é o CRA (Contramedidas para Radar Adaptativo). O objetivo deste programa é desenvolver capacidades de GE que possam combater o radar adaptativo inimigo (também chamado de radar digitalmente programável, um tipo de radar avançado capaz de detectar e compensar rapidamente possíveis bloqueios no equipamento, adaptando o modo operacional de transmissão/recepção em nano segundos.

3. METODOLOGIA

Será abordada nesta seção a metodologia utilizada durante o trabalho, descrevendo os tipos de pesquisa e classificações. O método usado para fazer a coleta de dados é descrito na seção 3.3 e por fim são realizadas observações referentes às limitações deste método.

3.1 Classificação da Pesquisa

O objetivo deste capítulo é apresentar a classificação da pesquisa quanto aos fins e quanto aos meios.

3.1.1 Classificação quanto aos fins

Inicialmente é realizada uma pesquisa exploratória de forma a realizar o levantamento bibliográfico sobre um tema e proporcionar mais informações sobre o assunto investigado, possibilitando sua definição e delineamento, além de definir os objetivos. Após uma análise exploratória do tema, optou-se pela pesquisa descritiva para observar, registrar, analisar e ordenar as informações. Buscou-se encontrar suas características, ocorrências e objetos relacionados.

O trabalho em questão possui uma metodologia cuja finalidade é aplicada e destina-se a possíveis aplicações na Marinha do Brasil para servir de subsidio aos meios navais que buscam evoluir e modernizar suas tecnologias de combate, com o intuito de embutir-se no moderno ambiente militar que o mundo se encontra.

3.1.2 Classificação quanto aos meios

É feita uma pesquisa bibliográfica com o intuito de levantar o conhecimento disponível sobre as tecnologias, técnicas e táticas que envolvam ataque eletrônico em aeronaves. O objetivo é conhecer a literatura já existente e formular uma proposta ou um pressuposto sobre o assunto. Buscar nas pesquisas, experiências ou estudos de caso e mencionar todas as possíveis aplicações para a MB

3.2 Limitações do Método

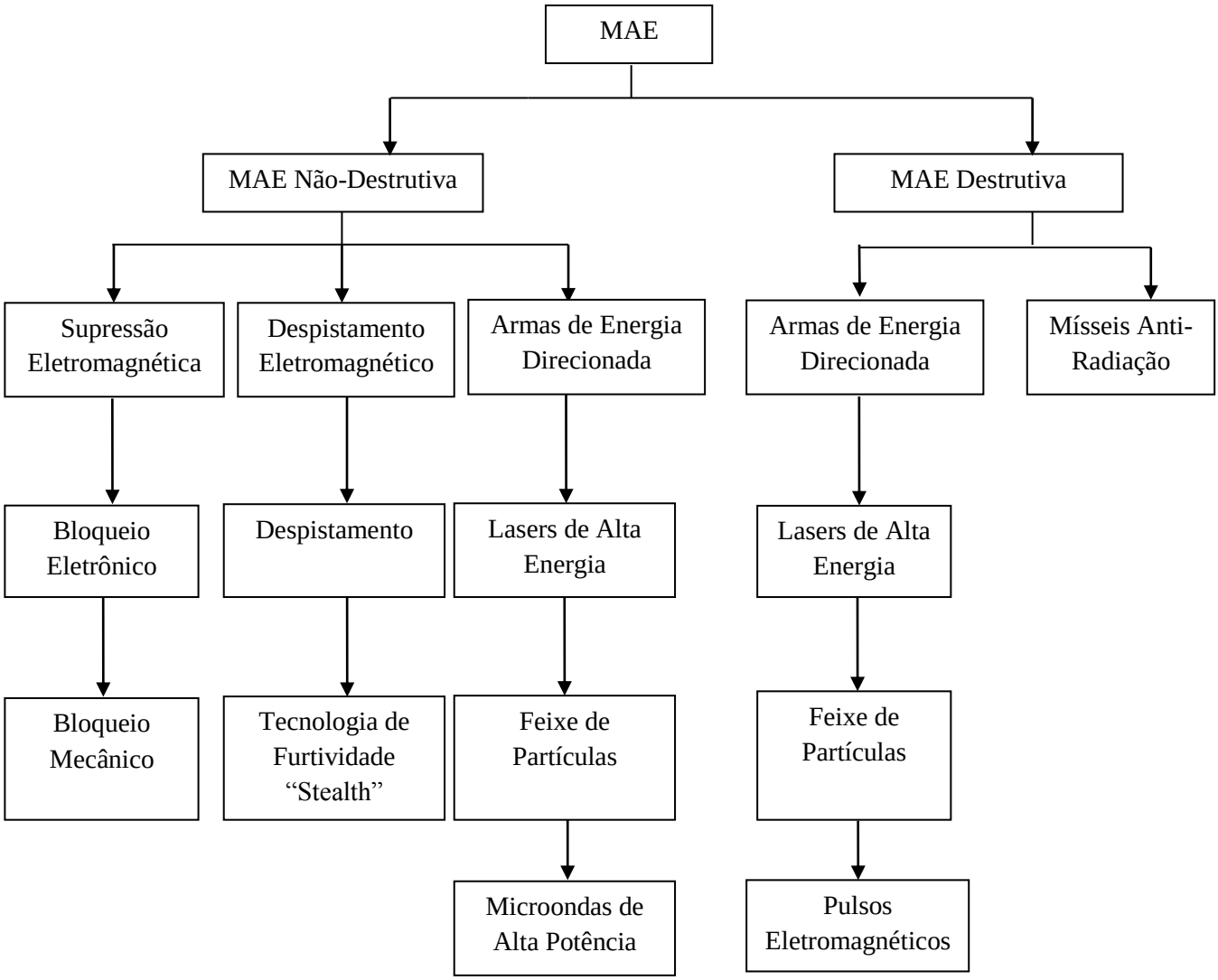
Conforme mencionado acima é realizada uma pesquisa bibliográfica para coletar informações em arquivos contidos em periódicos e documentos que aborde o tema. A metodologia adotada foi escolhida devido à circunstancias encontradas no momento pelo autor do trabalho, onde não existe tempo hábil para pesquisas em campo ou outras formas de se pesquisar o tema e buscar dados e informações de GE na Marinha do Brasil.

3.3 Coleta e Tratamento de Dados

As informações foram coletadas na pesquisa bibliográfica e buscaram-se documentos na forma de artigos publicados em jornais e revistas que abordassem as tecnologias que envolvam Medidas de Ataque Eletrônico (MAE) utilizadas na Guerra Eletrônica (GE) em situações de guerra aérea em diferentes situações de um combate. O foco maior foi dado em aeronaves americanas, uma vez que o país é uma das referencias em assuntos de GE e vem dominando essas missões nas ultimas décadas. Os dados observados Força Aeronaval da Marinha do Brasil possa se situar do atual patamar que se encontra perante as Forças Armadas de países desenvolvidos e que estão no estado da arte quando o assunto é GE.

4. TIPOS DE MEDIDAS DE ATAQUE ELETRÔNICO (MAE)

As MAE podem ser representadas conforme o diagrama abaixo. Basicamente, a divisão aborda medidas destrutivas e não destrutivas, ou seja, se o dispositivo irá destruir ou danificar sistemas eletrônicos inimigos ou se ele irá degradar por determinado tempo sua operação (FAB, 2011). Neste trabalho daremos ênfase apenas as MAE não destrutiva:



As seções seguintes realizam a abordagem de algumas dessas MAE detalhando as MAE não destrutivas.

4.1 MAE Não Destrutiva

As medidas de ataque não destrutivas podem ser divididas em bloqueio e despistamento por meio de técnicas com a finalidade de negar, neutraliza ou degradar momentaneamente o operação do inimigo.

4.1.1 Bloqueio e seus efeitos

Os equipamentos empregados nas medidas de ataque eletrônico utilizam técnicas fundamentais de interferência por ruído e despistamento. Algumas das principais técnicas utilizadas em operações aéreas serão abordadas e descritas de forma a demonstrar o objetivo operacional bem como os métodos de execução.

A distinção entre bloqueio mecânico e bloqueio eletrônico ocorre uma vez que, o primeiro é feito por meio do emprego de dispositivos que absorvem ou refletem radiação quando está posicionado entre transmissor e receptor. Por outro lado o bloqueio eletrônico participa de forma ativa utilizando-se de radiação intencional de energia eletromagnética para sobrepor o sinal de interferência ao sinal vítima (FAB, 2011).

Os sistemas de interferência por ruído são projetados para produzir perturbações em receptores de radares objetivando atrasar ou negar a detecção de alvos. As técnicas que empregam interferência por ruído podem ser empregadas em táticas de apoio e suporte a outras aeronaves ou mesmo para auto- proteção. Será descrito nesta seção algumas técnicas comuns de interferência por ruído como ruído de barragem (“barrage noise”), ruído de banda estreita (“spot noise”) e interferência por ruído modulado (“modulated noise”).

4.1.2 Bloqueio por ruído

Os sistemas de bloqueio por ruído são dispositivos de ataque eletrônico cuja finalidade é gerar um distúrbio no receptor do radar de modo a impedir a detecção de um alvo. Dentre os fatores mais importantes para quantificar a eficácia desse tipo de bloqueio está a relação de interferência-sinal (J/S). A relação J/S compara a potência do sinal de interferência gerado pelo equipamento de ataque eletrônico (jammer) com a potência do eco do alvo (sinal). A equação abaixo é uma expressão da relação J/S (USAF, 2000).

$$\frac{J}{S} = \frac{P_J G_J}{P_T G_T} x \frac{4\pi R^2}{\sigma}$$

P_J = potência transmitida pelo equipamento de ataque eletrônico

G_J = ganho da antena do equipamento de ataque eletrônico

P_T = potência de pico transmitida pelo radar

G_T = ganho da antena do radar

R = distância do alvo

σ = secção reta do alvo

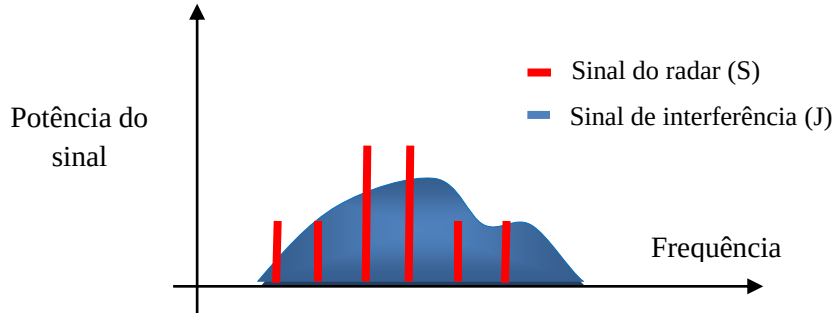
O autor salienta que o calculo da relação J/S considera para efeito de cálculo os parâmetros na saída do receptor do radar, de forma que o ganho do processamento do sinal do receptor seja aplicado ao sinal de interferência.

A distância do alvo é um ponto crucial na relação J/S e também na relação entre o sinal-ruído (S/N) do radar. A relação S/N mede o desempenho do radar vítima, sendo assim uma medida da capacidade do radar para detectar alvos. A equação de S/N leva em consideração vários parâmetros dentre eles a distância “R” entre o jammer e o alvo. Esta distância impacta no cálculo da expressão S/N com o valor de “R” elevado a quarta potência do denominador. Isso se deve ao fato do sinal transmitido pelo radar viajar do seu transmissor para o alvo e voltar ao seu receptor. Por outro lado, a relação J/S é calculada usando “R” levado a segunda potência, dada a transmissão unidirecional do pulso de interferência para o receptor do radar da vítima.

A relação J/S deve ser maior que um para garantir a efetividade do jammer. Os radares inimigos, principalmente os de superfície, normalmente transmitem sinais de

maior potência que um sistema de interceptação aérea. Como mencionado acima, este sinal do radar deve percorrer o dobro da distância que o sinal de interferência no ar. Para longas distâncias do alvo, um jammer de baixa potência pode gerar uma relação J/S muito maior que um. Ao se aproximar do alvo, a distância "R" que o pulso do radar percorre diminui com um aumento correspondente de potência no eco do radar, tal fato reduz a relação J/S para um valor menor que um e o radar detecta o alvo (Figura 4.1). A distância entre alvo e jammer correspondente ao ponto onde isso o ocorre é chamada distância de Burnthrough e ocorre quando a potência do sinal do alvo refletido excede a potência do sinal de interferência. O conceito de distância de Burnthrough explica por que uma técnica de bloqueio perde sua eficiência à medida que a aeronave se aproxima do radar (USAF, 2000).

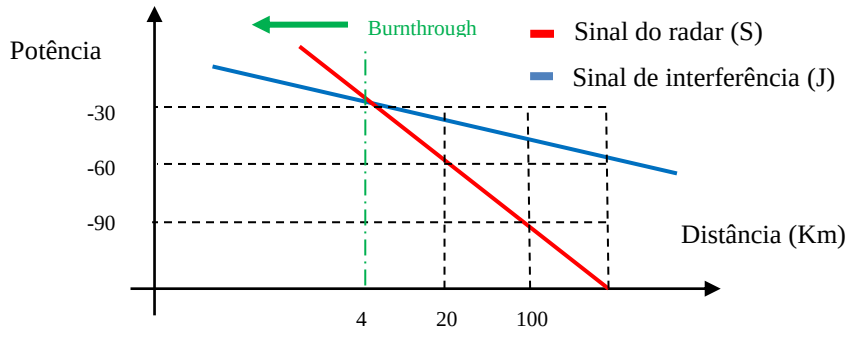
Figura 4.1 - Relação J/S < 1



Fonte: Elaborado pelo autor.

Ao traçar as potências do sinal do radar e do sinal de interferência versus a distância do alvo (Figura 4.2), esses dois valores se cruzam no ponto em que a relação J/S é unitária. Como pode ser visto, a curtas distâncias o sinal de interferência não está mais bloqueando o radar inimigo e a aeronave pode ser detectada.

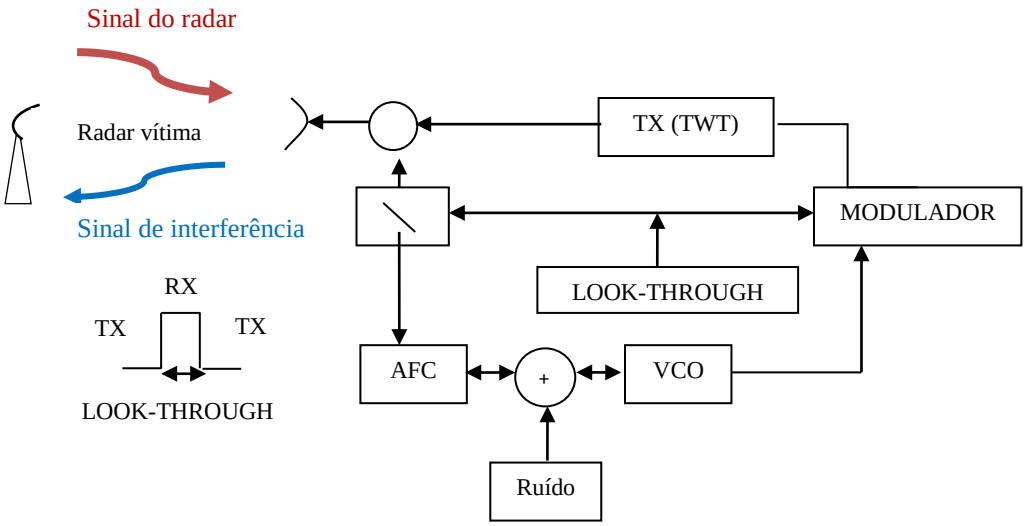
Figura 4.2 - Distância de Burnthrough



Fonte: Elaborado pelo autor.

No bloqueio a irradiação ou a reflexão deliberada de energia eletromagnética pode anular a efetividade de radares da força inimiga. A forma ideal de utilizar essa MAE é pela geração de ruído muito semelhante ao ruído térmico do radar da vítima, de modo que não haja detecção do sinal do alvo e de interferência. Ele depende de altos níveis de potência para saturar o receptor do radar e negar alcance e, ocasionalmente, informações de azimute e elevação para o radar da vítima. Nesta técnica aproveita-se a extrema sensibilidade do receptor do radar e o padrão de transmissão de sua antena para negar informações ao radar da vítima. O jammer pode ser representado por um receptor, um gerador de sinais de interferência e um transmissor. O receptor é necessário para identificar o sinal de interesse e para sintonizar o gerador de sinal de interferência na frequência correta. O sinal gerado é um ruído de uma dada largura de banda centrada na frequência do radar inimigo. Se as antenas receptoras e transmissoras não estiverem isoladas umas das outras, a sintonia é realizada durante os períodos de observação, quando a transmissão dos sinais de interferência é interrompida para que o sinal do radar da vítima possa ser recebido corretamente. Para não haver perda de eficiência, o período de visualização deve ser cuidadosamente determinado. A Figura 4.3 abaixo representa um diagrama clássico do gerador de ruído utilizado nas MAE.

Figura 4.3 – Diagrama do gerador de ruído



Fonte: (USAF, 2000, pag. 10-5).

Para compreender o diagrama deve-se entender o conceito de *look-through.* O termo corresponde as interrupções nos sinais de interferência, sendo uma técnica de observação com o objetivo de permitir que o jammer atualize os parâmetros de radar da vítima e mude o sinal de interferência para responder às mudanças nos parâmetros do sinal radar da vítima. Durante o *look-through* o dispositivo de controle automático de frequência (AFC) mantém um oscilador controlado por tensão (VCO) sintonizado na frequência do radar da vítima. Em seguida, o ruído é adicionado à tensão de sintonia do VCO para obter uma modulação aleatória na frequência do radar. O sinal resultante é enviado para um transmissor com amplificador de potência tipo TWT (traveling-wave tube), irradiando uma potência constante em direção ao radar da vítima (NERI, 2006, p. 383). Segue abaixo algumas características fundamentais de um sinal de interferência ou *jammer* (NERI, 2006, pag. 381):

- Área de cobertura
- Frequência excedente
- Sensibilidade do receptor
- Faixa dinâmica dos parâmetros aceitáveis para o receptor, incluindo largura mínima e máxima de pulso (PW) e frequência mínima e máxima de repetição de pulso (PRF)
- Largura de banda de ruído
- Qualidade do ruído
- Potência efetiva irradiada (potência transmitida multiplicada pelo ganho da antena)
- Polarização.

As seções seguintes abordam algumas das principais técnicas de bloqueio por ruído utilizado durante as missões de ataque eletrônico em operações militares.

4.1.3 Barrage noise

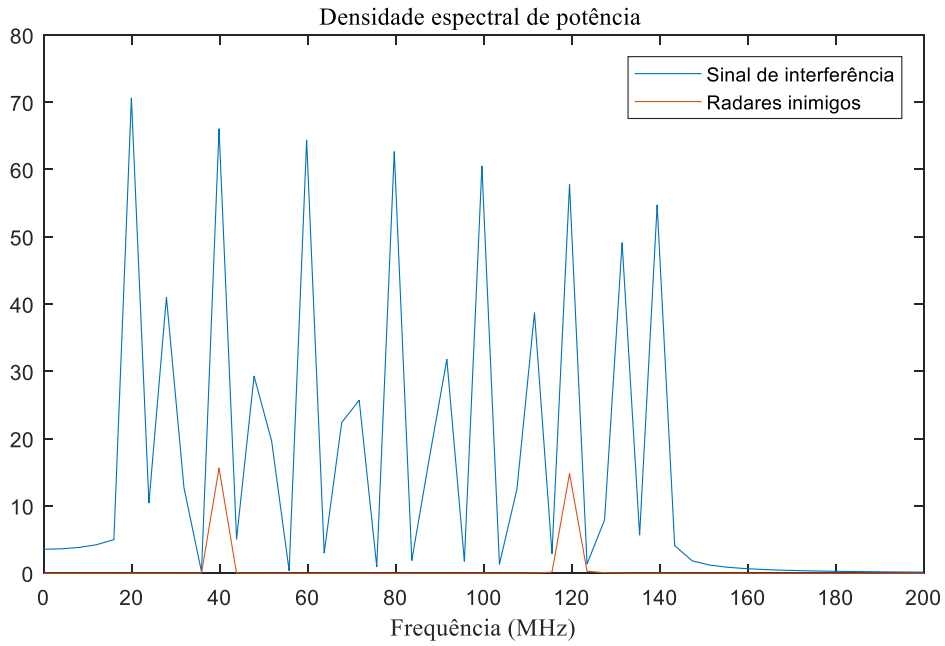
A idéia do ruído de barragem "*barrage noise*" é produzir um ruído de banda larga que cubra toda a largura de banda usada por um radar inimigo, principalmente os radares que possuem agilidade em frequência (Neri, 2006).

O conceito de densidade de potência deve ser mencionado para compreender que a eficácia da interferência por ruído depende da forma como a potência do sinal é distribuída pelas diferentes frequências. Basicamente, a densidade de potência em questão é uma função da largura de banda do sinal de interferência.

Quando um *jammer* caracteriza-se por uma banda estreita, ele consegue concentrar energia em uma faixa de frequência curta. Caso o *jammer* tenha uma banda mais larga e cubra uma ampla faixa de frequência, a energia gerada é distribuída por todo o espectro. Já que o jammer é caracterizado por uma energia irradiada fixa, ocorre a redução da potência efetiva de interferência para certa frequência.

Portanto, o bloqueio de barragem é uma técnica que sacrifica a transmissão em alta potência para que se transmita em várias frequências de radar. A Figura 4.4 ilustra por meio de um diagrama espectral de potência este método de interferência simulando um ruído de barragem atuando em frequências diferentes, cujo os valores são 40MHz e 120MHz. A distribuição do sinal de interferência em uma ampla faixa de frequência reduz a potência efetiva irradiada (ERP). Os equipamentos que utilizam esta técnica são de simples implementação e podem cobrir uma ampla faixa do espectro eletromagnético. Entretanto, a baixa densidade de potência influi negativamente nas situações que exijam alta relação de interferência/sinal (J/S) (USAF, 2000).

Figura 4.4 – Ruído de barragem



Fonte: Elaborado pelo autor.

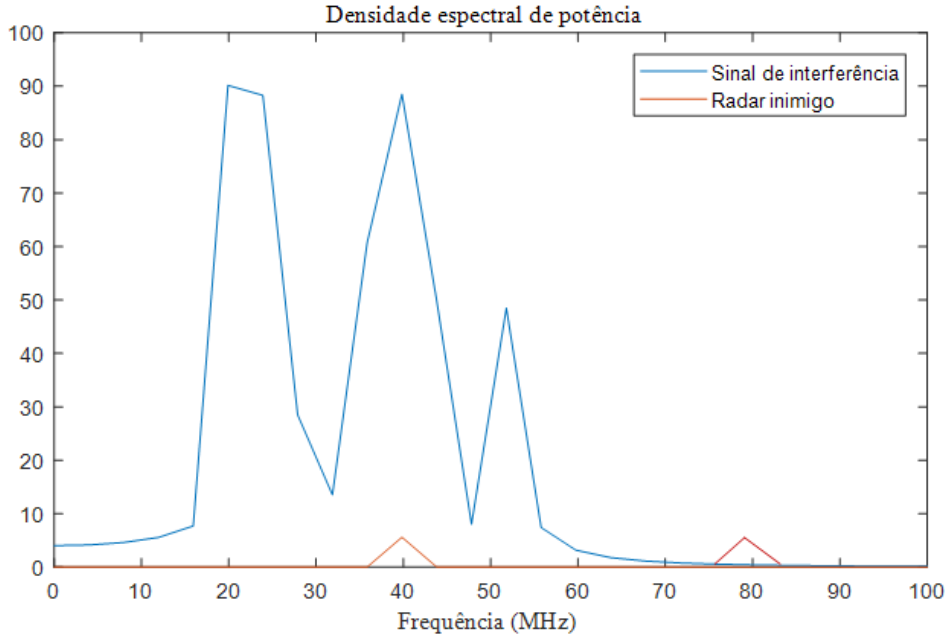
4.1.4 Spot noise

O ruído de banda estreita "*spot noise*" é um ruído com largura de banda limitada para cobrir o espectro do sinal irradiado pelo radar inimigo. A frequência central fica em torno da frequência do radar inimigo, sendo assim caso haja mudanças na portadora de RF a técnica pode ser ineficaz (USAF, 2000).

A técnica consiste em aumentar a potência do sinal interferente para a curta faixa de frequência do radar inimigo. Quando é necessário interferir em vários radares, automaticamente muitos *jammers* são requeridos. Contra sistemas modernos como os que possuem agilidade em frequência isso pode trazer problemas de transporte do equipamento em combate.

A alta densidade de potência do ruído de banda estreita é vantajosa uma vez que os radares inimigos podem sofrer interferências mais longas do que um ruído de barragem que possua mesma potência, como mostra a Figura 4.5. Em contrapartida a largura de banda limitada obriga que o operador manipule e sintonize constantemente o sinal de interferência na frequência do radar inimigo. Isso também pode se tornar complexo contra radares com agilidade em frequência.

Figura 4.5 – Ruído de banda estreita



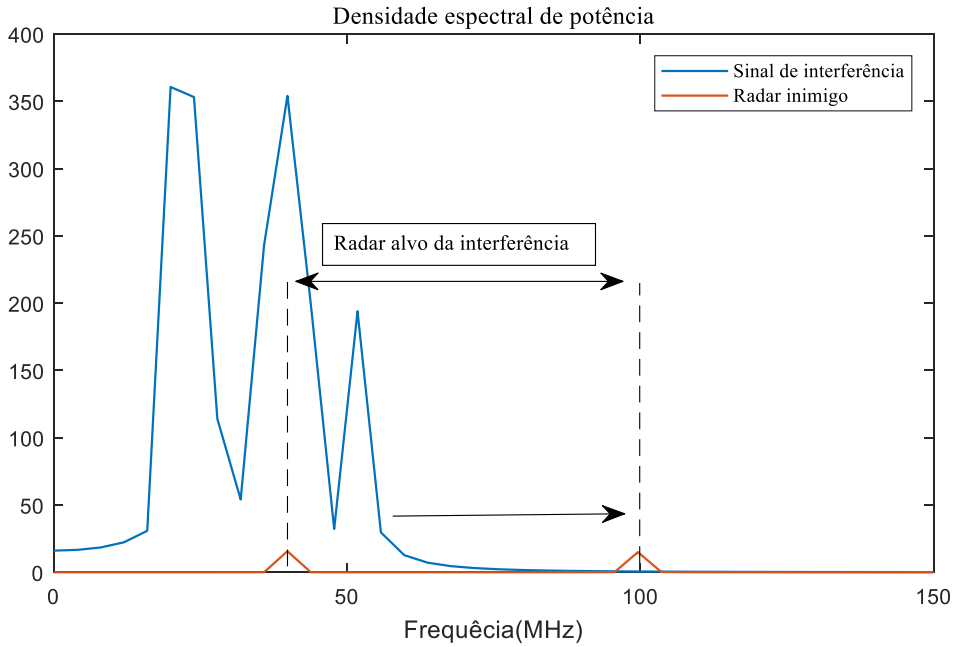
Fonte: Elaborado pelo autor.

4.1.5 Swept spot

O swept-spot é uma técnica utilizada quando uma alta densidade de potência é necessária de forma a atuar em uma grande largura de banda. Isso é feito por meio de interferência ruidosa capaz de varrer uma ampla faixa de frequência em diferentes velocidades, como mostra a Figura 4.6. Diferentemente do *barrage noise*, esta técnica preserva a alta densidade de potência e permite que o ruído cubra uma grande largura de banda, cobrindo vários sistemas radar (USAF, 2000).

O fenômeno conhecido como “ringing” pode causar oscilações de sinal dentro do receptor radar, principalmente em situações onde a interferência gerada ocorre com altas taxas de varredura, sendo assim deve-se atentar a velocidade utilizada para varrer as diferentes frequência do sinal de interesse. O que determinará a eficácia do swept-spot é basicamente a potência do sinal de interferência, a sua largura de banda e por fim a taxa de varredura desse sinal.

Figura 4.6 - Ruído *swept-spot*



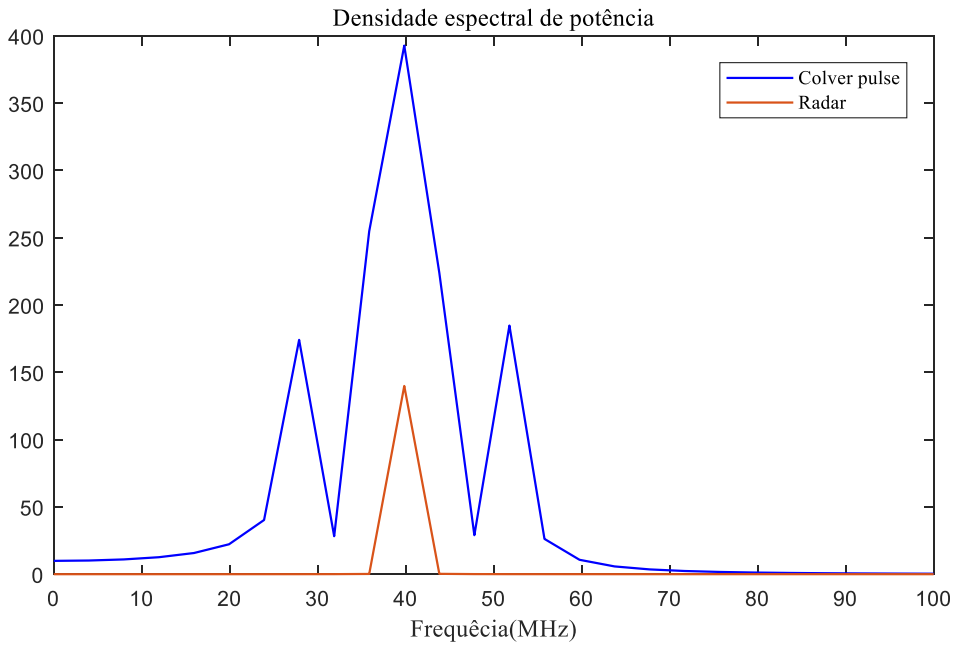
Fonte: Elaborado pelo autor

4.1.6 Cover pulse

O *cover pulse* consiste em uma técnica de “ruído inteligente” caracterizada pela modificação do swept-spot, atuando em curto intervalo de tempo, representado na Figura 4.7.

O receptor do jammer atua como um *transponder*, responsável por receber vários pulsos de radares e determinar a frequência de repetição dos pulsos (PRF) do inimigo. Assim, é possível mensurar o momento que o próximo pulso de radar deve chegar. Baseado nesses instantes de tempo, um oscilador atua transmitindo sinal ruidoso modulado e amplificado. Para ser aplicada com sucesso a técnica deve ser empregada contra radares de PRF fixa (USAF, 2000).

Figura 4.7 – Cover pulse



Fonte: Elaborado pelo autor

O *cover pulse* é o princípio de funcionamento da técnica de interferência por despistamento conhecida como "range gate pull-off" (RGPO). Neste caso, o equipamento responsável pela MAE transmite um sinal de interferência muito mais forte que o eco desejado, funcionando como um alvo falso que pode capturar o controle automático de ganho do radar. O tempo de atraso é aumentado no pulso de interferência e move a porta de acompanhamento para longe do alvo real.

4.1.7 Modulated noise

O ruído modulado, *modulated noise,* é uma técnica que pode usar ruído modulado em amplitude ou frequência e é empregada contra radares de

acompanhamento. O bloqueio de ruído modulado provou ser eficaz contra radares de varredura cônica e track while-scan (TWS) TTRs (USAF, 2000).

A frequência do sinal interferente é alterada conforme a taxa de varredura do radar inimigo. Portanto, contra um radar de varredura cônica é utilizado um sinal senoidal com frequência levemente maior que o radar alvo. A diferença de amplitude implica em uma variação de fase constante entre os sinais de interferência e do radar. Por meio dessa diferença de fase são criados alvos falsos de grande amplitude de sinal.

4.2 Despistamento e seus Efeitos

O principal objetivo do despistamento é fornecer ao radar vítima, informações erradas, para confundir o inimigo por meio da geração de sinais que são similares aos que o radar espera, mas com potência maior. Os sistemas de despistamento são capazes de receber e memorizar um sinal de radar e assim retransmiti-lo no momento apropriado, com modulações de amplitude, fase e polarização adequada. (NERI, 2006).

4.2.1 Despistamento por múltiplos alvos falsos

É uma técnica empregada para confundir um radar de busca ou um radar de acompanhamento durante a busca por alvos. A técnica de alvos falsos pode ser empregada tanto para missões de auto-proteção quanto para "stand-off". A intenção deste tipo de interferência é confundir o operador do radar inimigo gerando vários ecos de alvos falsos na PPI inimiga. Nas situações onde o alvo falso é empregado corretamente, o operador de radar não consegue diferenciar entre o alvo falso e o real.

A técnica em questão é empregada ao sintonizar o sistema de MAE com a frequência do radar inimigo, bem como a sincronização com a PRF e a taxa de varredura do radar da vítima. O pulso de interferência deve aparecer no radar alvo exatamente como um eco de radar de uma aeronave. Este eco é gerado com variações radiais e angulares quando o equipamento de MAE identifica o lóbulo lateral do radar e sincroniza o sinal com o lóbulo principal da vítima. Alvos falsos próximos são gerados antecipando a chegada de um de radar e transmitindo um pulso de interferência antes que o pulso de radar da vítima atinja a aeronave. Caso o radar da vítima possua uma

PRF variável, os sinais falsos podem ser gerados apenas a uma distância maior que a existente entre o equipamento de MAE e a vítima.

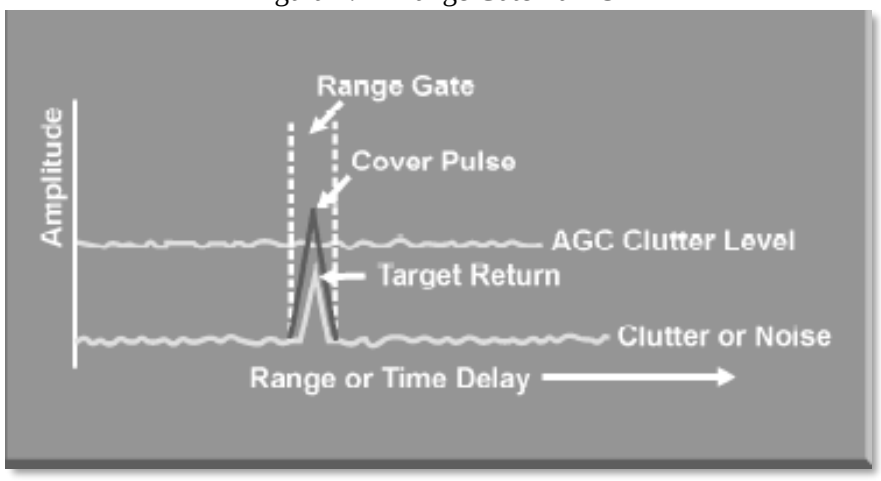
A criação de múltiplos alvos falsos é possível sabendo-se a frequência do radar da vítima, que é a variável utilizada para gerar a portadora de RF pelo equipamento MAE. Por meio de vários retardos são criados diferentes alvos falsos, sendo que preferencialmente devem ter velocidades maiores que o real para representarem maior potencial de ameaça.

4.2.2 Despistamento em distância - sistemas RGPO e RGPI

O "range gate pull-off" (RGPO) é uma técnica de despistamento que desloca a porta de acompanhamento em distância. O dispositivo de MAE recebe o sinal do radar e retransmite após introduzir uma série de atrasos. Ao perceber esses atrasos, o circuito de controle automático do ganho que está presente no radar inimigo aumenta o alcance movendo o alvo para uma distância falsa. O equipamento de despistamento é desativado quando o alvo falso atinge determinada distância. O radar de acompanhamento alvo da medida de ataque eletrônico perde o alvo e volta para o processo de aquisição.

O "range gate pull-in" (RGPI) também é uma técnica de despistamento que desloca a porta de acompanhamento em distância. No entanto a porta de acompanhamento é aproximada para enganar o radar da vítima. Para implementar este método é necessário conhecer o intervalo de repetição de pulso (PRI) bem como prever o tempo de chegada do pulso seguinte do radar da vítima para que o sistema de MAE possa emitir um pulso falso em intervalo de tempo planejado.

Figura 4.7 - Range Gate Pull-Off



Fonte: (USAF, 2000, pg. 10.9)

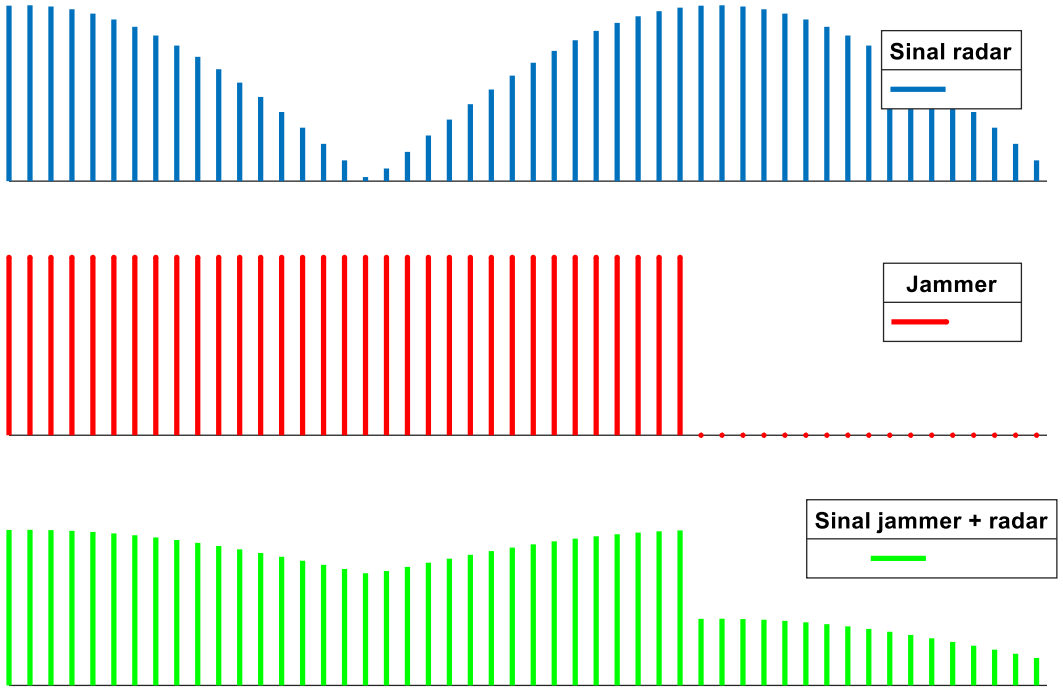
4.2.3 Despistamento em ângulo

O despistamento em ângulo é projetado para explorar possíveis vulnerabilidades durante o rastreamento angular do radar da vítima. Para empregar esta técnica de forma específica é necessário conhecer a metodologia de rastreamento que o radar alvo utiliza na obtenção de informações de azimute e elevação. Como exemplo será abordado três formas de despistamento aplicadas conforme o tipo de radar que se quer interferir.

A primeira delas é a aplicada contra os radares "track while scan" (TWS), onde a principal técnica de despistamento é a modulação em amplitude inversa. O TWS realiza o rastreamento em azimute e elevação de um alvo por meio de modulação em amplitude. O jammer de modulação de amplitude inversa gera um sinal com modulação exatamente oposta ao retorno esperado. O equipamento de MAE responde este radar, de forma sincronizada, por meio de um sinal com mesma frequência, PRF e taxa de varredura, mas com o inverso do padrão da antena do radar. Dessa forma são introduzidos erros na porta de rastreamento de ângulos do radar alvo, ocasionando a perca do rastreamento do ângulo.

Outra forma de despistamento utilizada contra radares de varredura cônica emprega *interferências de ganho inverso*. Uma vez que estes radares de varredura cônica utilizam a fase do sinal alvo, a técnica de ganho inverso tenta alterar a fase e a amplitude do sinal induzindo sinais falsos aos radares inimigos. Novamente, obtém-se a frequência, a PRF e a taxa de varredura do radar da vítima para que o equipamento de MAE transmita um sinal defasado 180° do alvo real, conforme a Figura 4.8.

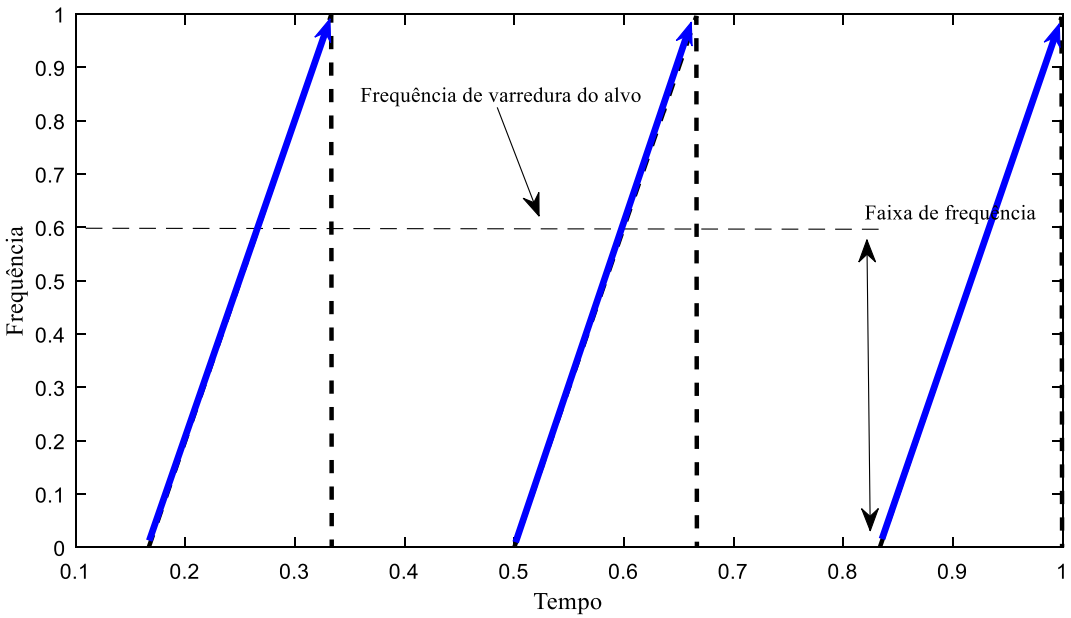
Figura 4.8 – Exemplo de interferência de ganho inverso



Fonte: Elaborado pelo autor

Por fim, a técnica de *interferência de onda quadrada (SSW)* é usada contra radares de busca “Lobe-On-Receive-Only” (LORO). Os radares LORO podem ser entendidos como um modo operacional de radar que pode ser implementado em qualquer radar com capacidade de buscar alvos de forma passiva. A idéia consiste em transmitir um sinal contínuo por meio de antenas que iluminam o alvo. O eco retorna para a plataforma e é recebido por um conjunto de antenas. A principal vantagem desses radares é a dificuldade de atuação eficaz por parte de sistemas inimigos de bloqueio e despistamento, uma vez que a antena que ilumina o alvo não tem taxa de varredura. A SSW consiste em criar pulsos de interferência com frequência variando continuamente durante a modulação em amplitude. O intervalo varrido por essa frequência é determinado por sistemas de inteligência eletrônica e o objetivo é induzir erros no *loop* de rastreamento de ângulo do radar LORO. (USAF, 2000).

Figura 4.9- Interferência de onda quadrada *(SSW)*



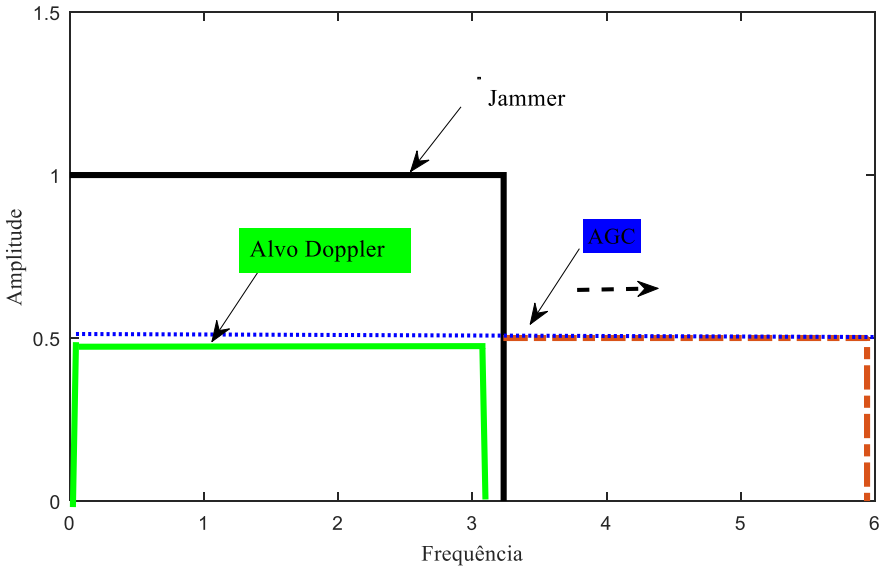
Fonte: Elaborado pelo autor

4.2.4 Despistamento em velocidade

O despistamento em velocidade objetiva negar informações de velocidade e gerar alvos com valores falsos de velocidade. A técnica de deslocamento da porta de acompanhamento em velocidade, "velocity gate pull-off" (VGPO) é utilizada contra radares Doppler pulsado ou radares de onda contínua (CW) e será abordada no trabalho para exemplificar este tipo de despistamento.

Os radares Doppler pulsado rastreiam os alvos com base no deslocamento Doppler, ou seja, sempre que existir variação na distância entre plataforma e alvo haverá *efeito Doppler*. Sendo assim, o VGPO captura a porta de acompanhamento automático de ganho (AGC) transmitindo um sinal CW com potência maior que o sinal de eco do radar e utilizando frequência Doppler aproximadamente igual ao sinal deste radar. Para enganar o inimigo, a frequência do sinal falso é alterada, movendo a porta de acompanhamento de velocidade (que inicialmente estava sintonizada nos valores reais) e induzindo valores falsos de velocidade, Figura 4.10, (USAF, 2000).

Figura 4.10 – Exemplo de técnica *VGPO*



Fonte: Elaborado pelo autor

4.3 MAE Destrutiva

O conceito de medidas de ataque eletrônico destrutivas é recente quando comparado as MAE não destrutivas. São consideradas formas de ataque eletrônico avançadas e tornaram-se efetivas em conflitos recentes (FAB, 2011).

A evolução tecnológica aliada pela indústria do conhecimento e contínuo progresso de sistemas digitais trouxe grandes desenvolvimentos para os sistemas de armas empregados atualmente. Como exemplo existe as armas de energia direcionada. O termo *energia direcionada* pode abranger tecnologias relacionadas à produção de um feixe de energia eletromagnética concentrada ou partículas atômica/subatômicas.

As armas de energia direcionada são compostas basicamente por: lasers, micro-ondas de alta potência (HPM)/radiofrequência (RF), que irradiam energia eletromagnética no alto espectro de RF e, por fim, os dispositivos de feixe de partículas que usam um grande número de fontes atômicas ou subatômicas.

Sendo assim, as armas de energia direcionada oferecem vantagens sobre as armas convencionais, proporcionando características como (DEVECI, 2007):

- ataque na velocidade da luz,
- alta precisão no direcionamento
- engajamento rápido de múltiplos alvos

- flexibilidade para ajustar o dano
- baixo custo operacional e,
- suporte logístico reduzido

No próximo capítulo, serão abordados no trabalho alguns dispositivos de ataque eletrônico que usam a energia direcionada como forma de ataque.

5. TIPOS DE MAE UTILIZANDO BLOQUEIO E DISPOSITIVOS MAE

As Medidas de Ataque Eletrônico podem ser classificadas conforme as táticas de bloqueio empregadas durante as operações militares que empregam a GE. As táticas são distintas de acordo com o posicionamento do meio (aeronave que realiza a interferência) em relação ao alvo, a fim de realizar o ataque eletrônico no radar vítima. As seguintes táticas serão abordadas:

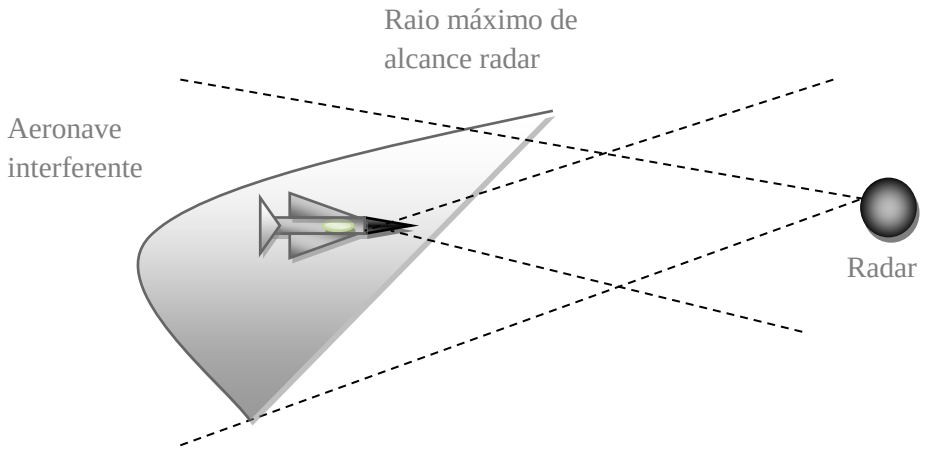
- Self-Protection Jamming (SPJ)
- Standoff Jamming (SOJ)
- Escort Jamming (EJ)

5.1 Self-Protection Jamming (SPJ)

O SPJ é caracterizado por equipamentos de ataque eletrônico instalados na plataforma onde se pretende realizar a defesa. A plataforma em questão pode ser uma aeronave, navio ou em terra, empregando técnicas de ruído ou despistamento por interferência (NERI, 2006).

Essa tática de auto-proteção pode ser considerada o tipo de MAE mais comum dentre as empregadas na GE de uma operação aérea, tendo como principal objetivo a sobrevivência individual da aeronave detentora do sistema de ataque eletrônico. O conjunto que compõe o sistema de bloqueio em questão pode ser composto por dispositivos como; “pod”, “chaff”, “flare” e em alguns casos sistemas com “towed decoy”. A finalidade é atingir o radar vítima de forma a quebrar o “track” do equipamento durante a busca por contatos ou até mesmo gerar erros de rastreamento até o radar perder o alvo (USAF, 2000). A Figura 5.1 ilustra de forma simplificada a SPJ realizada por uma aeronave diante de um radar vítima.

Figura 5.1 – Tática de Self-Protection Jamming (SPJ)



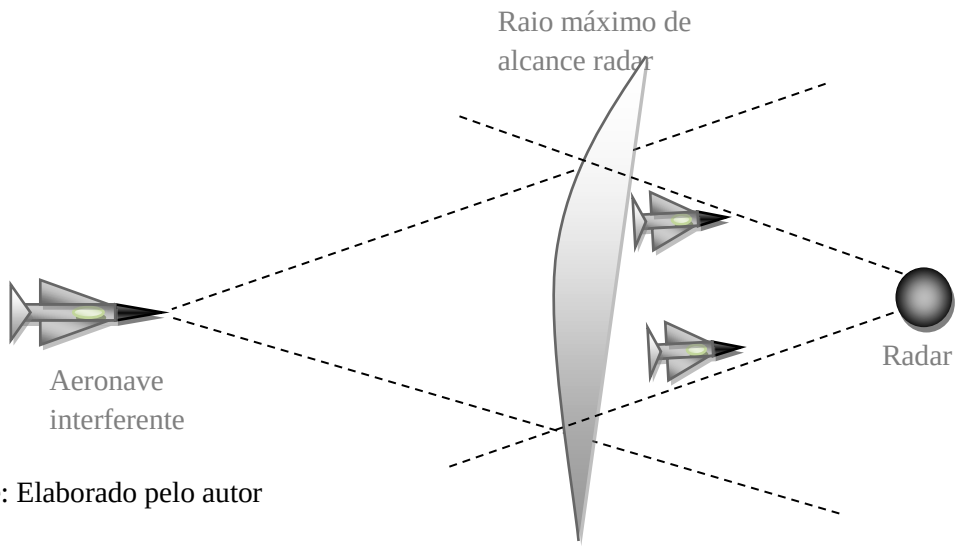
Fonte: Elaborado pelo autor

Normalmente, a tática de SPJ utiliza técnicas de interferência por despistamento. Isso se deve ao fato do despistamento requerer menos potência quando comparado a interferência por ruído. O menor gasto de energia significa menos peso e redução de espaço ocupado na aeronave, o que é relevante durante as operações aéreas. Por fim, o despistamento também é vantajoso por possuir capacidade de bloqueio contra múltiplas ameaças (USAF, 2000).

5.2 Standoff Jamming (SOJ)

A tática de bloqueio SOJ trabalha de forma que o equipamento de MAE fique instalado a bordo de uma plataforma situada distante da região de defesa. Nesta forma de bloqueio o objetivo é confundir radares inimigos, localizados em linhas de defesa aérea distantes, para que ocorra a incursão em território inimigo de forma segura, sendo assim a técnica utilizada é de interferência por ruído. (NERI, 2006).

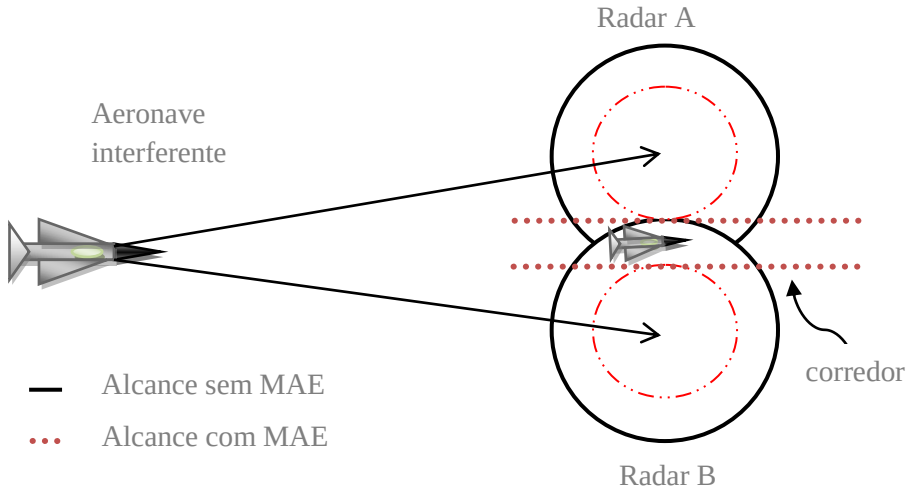
Figura 5.2 - Standoff Jamming (SOJ)



Fonte: Elaborado pelo autor

As plataformas localizadas fora das zonas de perigo dos sistemas de armas do inimigo apresentam sistemas de MAE que empregam a tática de "standoff" com alta potência de ruído. A radiação deve penetrar através dos lóbulos laterais das antenas de recepção dos sistemas de armas inimigos. Associa-se a essas plataformas um sistema de MAGE com capacidade para localizar e identificar os possíveis alvos e um sistema que possui capacidade para avaliar a letalidade de cada emissor localizado e alocar os recursos de MAE. (CIAW-322)

Figura 5.3 – “Corredor” de penetração criado pela SOJ



Fonte: Elaborado pelo autor

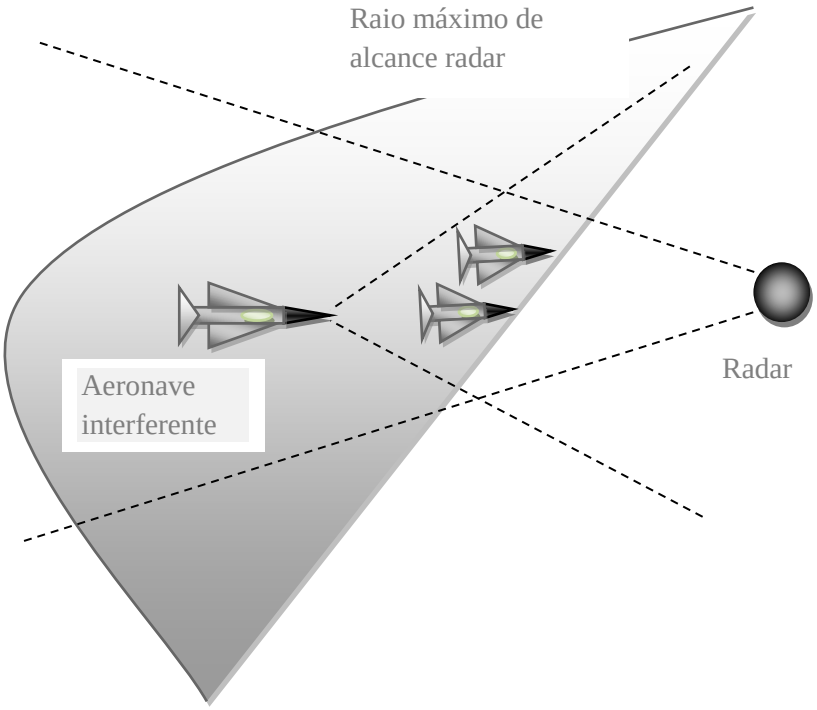
Nos últimos anos, levando em consideração os avanços do radar, reconheceu-se que a técnica de interferência de ruído não seria adequada às técnicas de radares que utilizam modulação de pulso (modulation on pulse - MOP) ou pulsos doppler. Por esta razão, a geração de sinais de despistamento contra os radares de busca é considerada mais eficaz do que os sinais de ruído. Caso o receptor do radar utilize a técnica CFAR (monitorar constantemente o ruído e ajustar o limiar de detecção de modo a manter uma taxa de falso alarme constante na entrada do acompanhador automático para que este não seja sobrecarregado com ecos falsos), mascarando a forças amigáveis a distâncias relativamente curtas do radar, uma alta potencia efetiva irradiada de ERP é necessária. A geração de múltiplos alvos falsos, de modo que o limite CFAR não é gerado, pode saturar os canais de rastreamento de radar de busca. (NERI, 2006).

5.3 Escort Jamming (EJ)

Na tática de Escort Jamming (EJ), a aeronave interferidora voará em conjunto com as demais aeronaves da esquadrilha para penetrar no território inimigo. A mesma consideração feita para o SOJ se aplica, com algumas ressalvas:

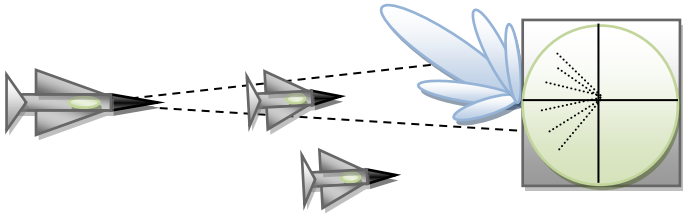
1- Se o jammer da escolta voar perto do inimigo, ele estará no feixe principal do radar ao mesmo tempo em que a plataforma (uma situação semelhante ao SPJ). Com isso, menor ERP e sensibilidade podem ser necessárias. Como a aeronave de acompanhamento tem que realizar as mesmas manobras que aeronaves protegidas, a cobertura do ângulo da antena deve ser muito ampla.
2- A aeronave que possui o equipamento de MAE de escolta acompanha as plataformas de ataque dentro da zona de combate e pode se tornar vulnerável. Normalmente esta forma de operar é usada quando a plataforma de ataque não tem potência, espaço, ou capacidade de carga útil suficiente para se proteger. A evidente desvantagem na tática de EJ é o risco da plataforma interferidora ser destruída e toda a força de ataque ficar desprotegida. As Figura 5.4 e 5.5 ilustram a tática de EJ aplicada para proteger duas aeronaves sobrevoando a área de detecção do radar vítima.

Figura 5.4 - Escort Jamming (EJ)



Fonte: Elaborado pelo autor

Figura 5.5 – Equipamento MAE atuando durante a EJ



Fonte: Elaborado pelo autor

Alguns dos principais equipamentos utilizados em MAE serão abordados no trabalho de forma sucinta a fim de se ter uma breve idéia de conceitos comuns na área de ataque eletrônico.

5.4- Chaff

O *chaff* é uma forma de MAE descartável amplamente utilizada em ataque eletrônico e é considerada uma arma eficiente na GE. O dispositivo *chaff* consiste em múltiplos dipolos metálicos de alta refletividade projetados para interferir e confundir a operação do radar vítima. Estes dipolos são lançados na atmosfera com a missão de impedir a aquisição, gerar alvos falsos ou até mesmo interromper o rastreamento de radares. O dispositivo é projetado para ser lançado a partir da aeronave e tem tempo de atuação limitada (USAF, 2000).
Além disso, outras características do *chaff* que podem ser ressaltadas são (FAB, 2011):

- Apresentar baixo custo para implementação;
- Característica inclusiva uma vez que pode atingir radar inimigo ou não;
- Não é possível controlá-la e tem ação até o espalhamento ou queda.

A evolução no desenvolvimento de radares modernos e a presença de um ambiente de GE com equipamentos cada vez mais robustos não resultou em desuso dos dispositivos chaff, que continuam sendo extremamente eficazes no ataque eletrônico. Durante uma tática de auto-proteção o equipamento pode ser utilizado para criar uma "saturação" na área de interesse ou criar um corredor de invisibilidade.

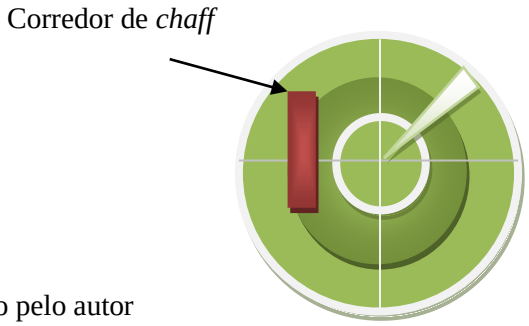
5.4.1 Corredores de *chaff*

O "corredor" de *chaff* é formado sempre que uma aeronave voa em linha reta e realiza o lançamento de forma contínua, formando "nuvens" consecutivas no de múltiplos dipolos metálicos presentes no ar (Figura 5.6). Caso haja rotas paralelas durante o vôo, o espalhamento do *chaff* pode criar uma grande área de cobertura envolvida pelo material.

Uma das formas de se utilizar o corredor é em situações onde se pretende mascarar uma incursão, uma vez que as aeronaves que voarem nas proximidades da nuvem, não poderão ser detectadas e acompanhadas. Outra aplicação do corredor de *chaff* é como despistamento, ao criá-lo em regiões diferentes da área de ataque. A presença dos *chaff* pode reduzir o ganho do radar no momento que

o equipamento varre a região, conseqüentemente haverá diminuição ou desaparecimento dos alvos mais fracos na região do corredor.

Figura 5.6- Corredor de *chaff* em display tipo PPI.



Fonte: Elaborado pelo autor

5.4.2- Aplicação contra radar de direção de tiro

No cenário atual de guerra, o uso de *chaff* para quebrar acompanhamento de um radar de direção de tiro é uma das formas mais comuns de aplicação destes dispositivos de GE. O mais importante nesta técnica é o tempo de lançamento utilizado na operação do ataque eletrônico. A quebra do acompanhamento acorre quando a nuvem de *chaff* atingir a RCS almejada a uma distância próxima da aeronave. Basicamente, as duas formas de se quebrar o acompanhamento destes radares são:

1- Seqüência de lançamentos

O lançamento sucessivo de nuvens de *chaff* é realizado para que o radar acompanhe momentaneamente a seqüência de nuvens. Quando o radar descartar uma dessas nuvens após perceber que não é um alvo, ele busca a nuvem consecutiva. Sendo assim, a missão é manter o alvo fora do eixo de acompanhamento do radar.

2- Limitações do servo mecanismo da antena

Por motivos de retardo no servo mecanismo da antena, durante a busca pelo alvo o feixe pode ultrapassar o contato por um determinado período de

tempo. Sempre que ele voltar para centrar o alvo, a aeronave pode lançar um *chaff*, realizando isso de forma consecutiva e aumentando o erro angular até que o radar perca o acompanhamento total.

5.5 Pod

Os dispositivos de defesa eletrônica em aeronaves podem ser internos, de forma que não são visíveis e localizando-se em compartimentos dedicados ou podem ser projetados para ficar em áreas externas a aeronave, os chamados POD. A configuração POD pode ser considerada como um sistema de interferência importante em situações onde não exista espaço interno a plataforma, sendo necessário projetar adaptações para posicionar o equipamento de GE. Nessas circunstancias, uma nova análise na aerodinâmica da plataforma é necessário a instalação do casulo. O dispositivo normalmente apresenta um contêiner aerodinâmico preso à aeronave por meio de estruturas, inicialmente destinados a transportar munições (Figura 5.7). A adaptação é útil quando os equipamentos de defesa eletrônica possuem dimensões que impossibilitam seu posicionamento interno a aeronave ou quando não há fonte de energia dentro da plataforma. (NERI, 2006)

Figura 5.7 – Sistema de MAE instalado na configuração POD em uma aeronave

A vantagem de sistemas POD está na possibilidade em se evitar sobrecarga na aeronave pelo peso do equipamento de defesa eletrônica em determinadas missões. Nas

missões de combate, a aeronave será forçada a renunciar de um dos pilares disponíveis para a cápsula.

Os PODs podem ser inseridos sob a fuselagem ou sob as asas da aeronave. Os dispositivos colocados sob a fuselagem normalmente são pesados e volumosos, porém o equipamento não sofre influência severa das condições ambientais. Por outro lado, quando os PODs são inseridos sob as asas, normalmente são menores e mais manobráveis, no entanto os componentes eletrônicos dentro delas devem suportar um severo regime de vibração, exigindo alta qualidade de fabricação do material da cápsula.

A aeronave com sistemas POD tem uma capacidade de vôo reduzida. A velocidade máxima admissível em função da altitude é menor que a de uma aeronave sem o dispositivo. (NERI, 2006)

No Brasil, a Força Aérea Brasileira (FAB) adquiriu o POD SKY-SHIELD para cumprir missões de supressão de defesa aérea. A aeronave tem como função atuar em missões de supressão da defesa antiaérea inimiga, capaz de interferir em todas as ameaças de um cenário de guerra moderno como as emissões de radar e mísseis. O equipamento pode realizar as seguintes táticas de interferência e despistamento (SANTOS, 2009):

- Stand-Off Jamming
- Escort Jamming
- Self-Screen Jamming

Algumas características do POD SKY-SHIELD são mencionadas abaixo:

- Capacidade de operar em três bandas: Low band, Medium band e High band;
- 360^{o} de cobertura na recepção;
- Capacidade de criar um corredor para a incursão de aeronaves em territórios inimigos;
- Realiza várias táticas de interferência/despistamento como: (Wide Band Noise (WBN); Combine Noise (CN); Narrow Band Noise (NBN), etc.

Figura 5.8 - Casulo Sky Shield da *Rafael*

Fonte: www.aereo.jor.br (2018)

Além disso, o POD SKY-SHIELD pode operar de forma autônoma ou controlada pelo piloto e também é caracterizado por uma alta ERP. (SANTOS, 2009).

Outros equipamentos de interferência que são largamente utilizados nas operações aéreas são: AN/ALQ-99, AN/ALQ-131, AN/ALQ 167 e ERIJAMMER A110. A tabela abaixo descreve de forma sucinta algumas características destes equipamentos e as Figuras 5.9 e 5.10 ilustra alguns desses equipamentos.

Tabela 5.1

Equipamento	Descrição
AN/ALQ-99	Intercepta e processa automaticamente os sinais radar e controla o seu sistema transmissor para interferir eficientemente em um grande número de ameaças radar com uma alta ERP. Realiza as táticas SOJ e EJ.
AN/ALQ-131	Sistema de auto-proteção automático e modular, desenvolvido para prover cobertura em banda larga, contra diversos tipos de radares responsáveis por guiar armamentos.
AN/ALQ 167	Possui capacidade de geração de ruído, despistamento e interferência. Sistema é completamente autônomo e realiza todas as funções de recepção, processamento e transmissão requeridas para interferir nos radares. Os parâmetros operacionais podem ser selecionados em terra, com a utilização da barra serial RS-422, ou controlados e modificados em tempo real durante a missão.
ERIJAMMER A110	Opera em dois modos: autônomo e controlável (operado pelo Oficial de Guerra Eletrônica - OGE durante a missão). Durante um engajamento típico, o OGE visualiza na DU símbolos que identificam a ameaça e alarma um alerta sonoro quando a ameaça é identificada como inimiga Na DU também é mostrada a distância estimada para a ameaça. O sistema tem a capacidade de look through durante a interferência, sendo o OGE alertado sempre que surge um novo emissor.

Figura 5.9 - AN/ALQ-131 utilizado nas aeronaves F-16, F-111, A-10, F-4, F-15, F-5 e C-130.

Fonte: www.aereo.jor.br (2018)

Figura 5.10 - AN/ALQ-167 jamming pods desenvolvido pela Rodale for NATO's Multiservice Electronic Warfare Support Group (MEWSG)

Fonte: www.aereo.jor.br (2018)

5.6 Decoy

O *decoy* é um dispositivo projetado para ser detectado pelo radar inimigo como se fosse a própria aeronave possuidora do equipamento, ou seja, assemelham-se com a plataforma que estão protegendo. Para que isso ocorra, o *decoy* deve possuir velocidade e RCS semelhantes à plataforma protegida. Como ele tem dimensões menores que as aeronaves, técnicas para aumentar a RCS devem ser empregadas (FAB, 2011).

As três missões básicas desses equipamentos são:

- saturar o sistema de defesa aérea integrado (IADS) do inimigo
- forçar o inimigo a expor suas forças prematuramente
- negar o rastreamento pelo radar inimigo

Os principais tipos de *decoy* que serão abordados são: “decoys de saturação”, “decoys rebocados” e “decoys descartáveis”.

5.6.1 *Decoys* de saturação

O *decoy* de saturação é um objeto descartável construído para simular uma aeronave que penetra na área de interesse, com missão de despistar e saturar o inimigo, Figura 5.11

Figura 5.11 – Decoy Miniature Air-Launched (MALD-J)

Fonte: www.aereo.jor.br (2018)

O lançamento de vários *decoys* de saturação força o inimigo a utilizar grande parte do seu armamento de detecção e ataque, o que pode gerar o esgotamento de seus recursos e permitir o engajamento de aeronaves (USAF, 2000). As três principais características desses dispositivos são:

1- *Assinatura eletrônica:* O *decoy* deve possuir uma assinatura eletromagnética igual a da aeronave que ele está protegendo, por meio de dispositivos construídos com tamanho, forma e material adequados para que o *decoy* irradie o mesmo sinal que é emitido pelo inimigo. A forma ativa consiste em sistemas com circuitos repetidores próprios capazes de coletar os dados do sinal do radar vítima, amplificá-los e retransmiti-los para o inimigo com características de tamanho adequadas de forma a confundir a vítima.

2- *Características do vôo*: A eficácia de um ataque eletrônico com este tipo de *decoy* também depende da semelhança de vôo com a aeronave que ele está protegendo, aumentando a probabilidade de que o dispositivo efetivamente engane o inimigo por um período de tempo adequado. Os *decoys* modernos podem conter sistemas de propulsão com foguetes ou pequenos motores e, em alguns dispositivos, as rotas de vôo podem ser pré-programadas e o equipamento pode voar de forma autônoma.

3- *Missão:* A missão de saturar o inimigo ao lançar um número significativo de *decoys*, podendo saturar ou sobrecarregar um sistema de defesa aérea integrado (*Integrated Aerial Defense System - IADS*). Além disso, ao atrair o inimigo por meio da assinatura eletromagnética assemelhada com a aeronave e rotas de vôo pré-programadas, os radares inimigos ficam expostos a identificação (forçar o inimigo a expor suas forças prematuramente).

5.6.2 *Decoys* rebocados

O *decoy* rebocado é formado por uma pequena estrutura jammer conectado a aeronave. Ele é projetado para proteção individual da aeronave de forma a garantir a sobrevivência da plataforma contra mísseis no estágio final do engajamento, sendo uma medida defensiva da aeronave. A principal missão é manter uma distância segura entre um míssil guiado por radar de forma semi-ativa e a aeronave contendo o dispositivo. Os radares doppler pulsado e monopulso também podem sofrer influência de *decoys* (USAF, 2000).

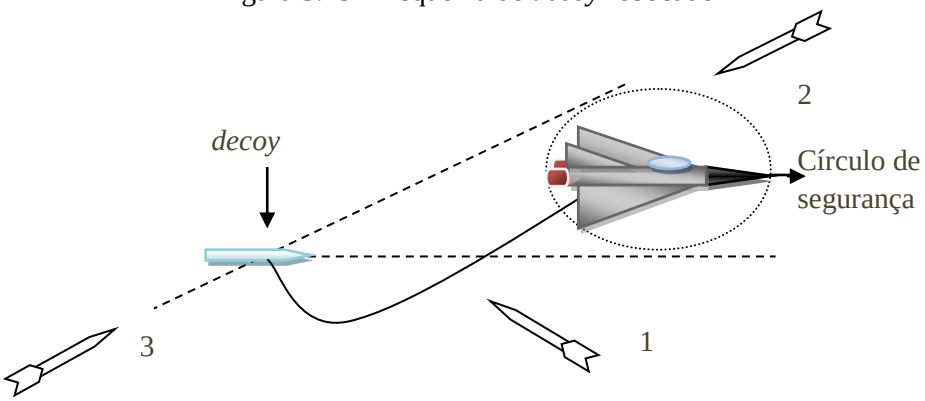
Figura 5.12 – Decoy rebocado AN/ALE-50 dentro do pod AN/ALQ-184

Fonte: www.aereo.jor.br (2018)

A Figura 5.13 demonstra três situações onde um *decoy* pode atuar durante um ataque. Na situação "1" tem-se a melhor situação no que se refere a geometria da cobertura angular, sendo assim o *decoy* atua de forma efetiva contra o míssil. Caso o míssil aproxime pela dianteira da aeronave, situação "2" da figura, pode ocorrer do armamento explodir antes de atingir o *decoy* e danificar a aeronave.

Por fim, na situação "3" o míssil se aproxima pela parte traseira da aeronave que utiliza o *decoy* rebocado e caso o míssil não atinja o dispositivo de despistamento, ele pode ir na direção da aeronave.

Figura 5.13 – Esquema de *decoy* rebocado



Fonte: Elaborado pelo autor.

5.6.3 *Decoys* descartáveis

O ataque eletrônico por meio de *decoys* descartáveis consiste em lançar objetos na forma de pequenos mísseis capazes de gerar sinais de despistamento para atrair as portas de acompanhamento da ameaça (NERI, 2006).

Para operar de forma eficaz o dispositivo enfrenta algumas dificuldades como: *frequência doppler* e *período de eficácia do sinal decoy*. A frequência doppler pode ser gerada transmitindo para o *decoy* uma frequência calculada. Quando o dispositivo de despistamento recebe este sinal com a frequência desejada (frequência doppler da aeronave que está sendo protegida), ele irradia o sinal para atrair a porta de velocidade do míssil anti-aéreo. A outra forma de resolver o problema da frequência doppler é o *decoy* descartável possuir um sistema independente capaz de gerar a frequência de

despistamento correta de forma autônoma. O segundo problema é a dificuldade encontrada pelo *decoy* em manter sua eficácia por muito tempo, já que ele é separado da aeronave. Assim, o lançamento do *decoy* deve ocorrer quando o míssil estiver se aproximando e na distancia correta da aeronave. Caso não tenha conhecimento das informações do inimigo, pode ser necessário lançar vários dispositivos de forma consecutiva, sendo assim necessário a aeronave estar equipada com muitos dispositivos deste tipo. A Figura 5.14 mostra um exemplar do decoy descartável ADM-20 da Força Aérea dos Estados Unidos.

Figura 5.14 - Decoy descartável *ADM-20*.

Fonte: www.aereo.jor.br (2018)

5.7 Flare

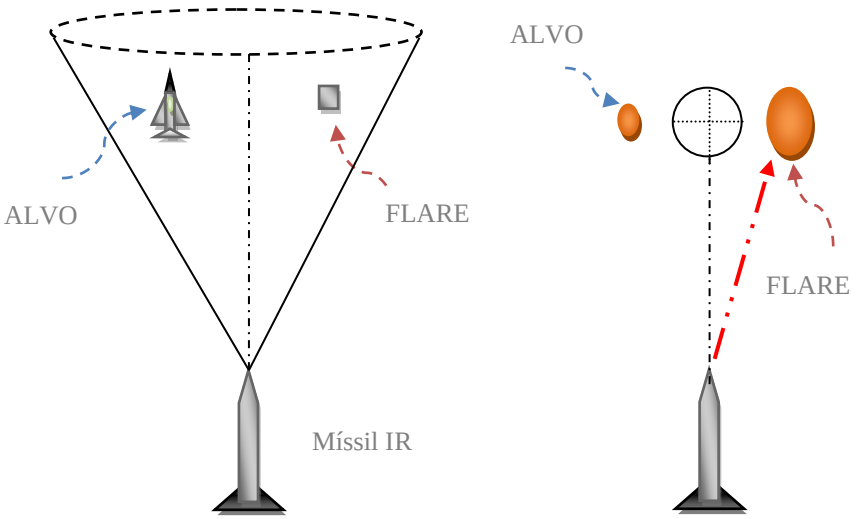
O desenvolvimento de avançados mísseis guiados por infravermelho acarretou na necessidade de combater ameaças IR diante do cenário da guerra atual. No contexto das MAE um dos principais dispositivos usados para o ataque eletrônico contra armamentos guiados por radiação infravermelha (IR) é o *flare.* O *flare* é um equipamento situado em cartuchos e pode ser armazenado no mesmo local que os dispositivos *chaff.* Após o lançamento e atuando por alguns segundos o equipamento é capaz de produzir radiação infravermelha maior que a plataforma protegida, atraindo o míssil inimigo (USAF, 2000). A tabela 5.7 descreve as principais características a serem consideradas durante o lançamento dos dispositivos *flare* (FAB, 2011).

Tabela 5.7 – Características do dispositivo *flare*

CARACTERÍSTICA	DESCRIÇÃO
Velocidade e ângulo de ejeção	representam a dinâmica de separação *flare*/plataforma.
Rise time	tempo necessário para que o *flare*, após a ejeção, atinja sua temperatura de efetividade
Temperatura de efetividade	menor temperatura que o *flare* deve atingir para se tornar um alvo atrativo para o dispositivo a ser atacado, simulando ou mascarando a assinatura IR da plataforma a ser defendida.
Espectro de emissão IR	tempo em que o flare é capaz de manter-se acima da temperatura de efetividade.
Duração da queima	tempo em que o *flare* é capaz de manter-se acima da temperatura de efetividade

A Figura 5.15 ilustra um míssil IR e seu campo de visada abrangendo uma área que contempla a aeronave e o *flare*. Inicialmente, o dispositivo deve provocar o direcionamento do míssil para um ponto intermediário entre alvo e o próprio *flare*. O equipamento MAE gera mais radiação IR que o alvo a ponto de atrair o míssil em sua direção. Após finalizar a queima do *flare*, a aeronave (alvo) deve estar fora do campo de visada do sistema de busca do míssil.

Figura 5.15- Aeronave e *flare* vistos por míssil IR. Conforme o lançamento o míssil é direcionado para o *flare*.



Fonte: Elaborado pelo autor.

5.8 Mísseis Anti-Radiação

O míssil antiradiação (MAR), conhecido também como ARM “antiradiation missile” é uma MAE destrutiva de alta precisão, o MAR é guiado pela radiação emitida por radar inimigo. A identificação do radar emissor ocorre através de um sistema passivo, capaz de extrair os dados angulares do radar. Os MARs têm grande importância em operações militares, essas armas de ataque eletrônico despertam muitas dúvidas quanto ao uso do radar pelo inimgo e é um fator de dissuasão (NERI, 2006, pag. 250).

Os MARs normalmente são mísseis lançados por plataformas aéreas e instalados a bordo de aeronaves utiizadas em missões de GE para realizar a supressão da defesa aérea inimiga (SEAD)
O míssil antiradiação interage com um sistema MAGE a bordo da aeronave que intercepta, identifica, e localiza o radar da vítima. Após a identificação realizada pela aeronave, o receptor do MAR processa essas informações contendo parâmetros como largura de pulso (LP), intervalo de repetição de pulso (PRI) e frequência da portadora e seu sistema de busca pode agora guiar-se pelo sinal do radar . Após o lançamento, o míssil não requer assistência (mísseis com orientação ativa).

Uma das forma de se proteger do MAR é o radar da vítima parar de transmitir, o que não garante a sobrevivencia do radar já que o míssil pode continuar rastreando com base em coordenadas computadas em sua memória. O radar pode alternativamente procurar a ajuda de um sistema de armas para destruir o míssil.

O Brasil entrou para o pequeno grupo que detém a tecnologia de MARs, estima-se hoje que menos de dez países são capazes de projetar e produzir tal arma. O *MAR-1* é o primeiro míssil antiradiação brasiliero, a arma é produzida pela Mectron, que realizou este ambicioso projeto desde 1998 em conjunto com o DCTA. Segundo (MULLER, 2013) a Força Aérea Brasileira utilizará o míssil nos caças AMX A-1 e Brasil irá exportar a arma para o Paquistão, que assinou contrato para a aquisição de 100 mísseis em 2008 e já possuindo a arma integrada em suas aeronaves JF-17, Mirage III e Mirage V.

Figura 5.16- Míssil anti-radiação *MAR-1*

Fonte: www.aereo.jor.br/2013/12/12/contrato-com-paquistao-avanca-na-mectron (2018)

5.9- Dispositivos de energia direcionada

As armas de energia direcionada são dispositivos que empregam fontes de energia eletromagnética para causar danos diretos ou destruição de equipamentos, instalações e pessoal inimigo, ou para determinar, explorar, reduzir ou impedir o uso inimigo do espectro eletromagnético através de danos, destruição e interrupção (DEVICI, 2007). Além disso, inclui ações tomadas para proteger equipamentos e instalações de pessoal.

Figura 5.17 – Arma de Energia Direcionada em diferentes plataformas

Fonte: (DEVICI, 2007, pag. 6)

O interesse pelas armas de energia direcionada ocorre devido às vantagens encontradas nesse tipo de armamento cujas vantagens são enumeradas abaixo (DEVICI, 2007):

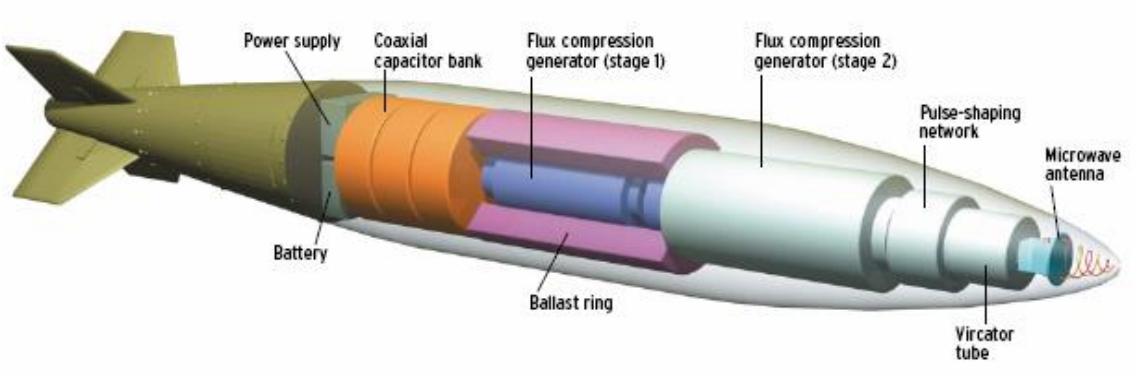
1- Fornecimento de energia letal na velocidade da luz, o que permite atuação instantânea a alvos rápidos e manobráveis. Como não há tempo entre disparar uma arma de energia direcionada e seu impacto com o alvo, os problemas associados à pontaria e descarga de armas são eliminados.
2- O fato de a energia ser ajustável contribui quando a opção de impor ataques não letais antes do uso de força letal. Diferentemente de armas químicas que podem ter efeitos devastadores e não intencionais, as armas de ED permitem flexibilidade de engajamento, conforme a potência transmitida e o tempo de irradiação, tornando as armas de ED valiosas.
3- As armas de ED são extremamente precisas. A parte específica de um alvo pode ser atacada, mesmo ele movimentando-se rapidamente, permitindo intervenções precisas sem a ocorrência de danos colaterais.
4- As armas de ED também se caracterizam pela indiferença que os feixes de energia direcionada possuem com relação à gravidade. A ausência de massa resulta na eliminação de restrições cinemáticas e aerodinâmicas que limitam as armas tradicionais.
5- Os sistemas de ED demandam grandes investimentos para desenvolvimento e construção, mas os custos após esses estágios podem ser mínimos, porque esses sistemas de armas gastam apenas energia.

Como foi abordado em (FAB, 2011), a tecnologia de ED tem aplicações em armas como bombas, cabeça de combate de um míssil e canhões embarcados em aeronaves ou veículos terrestres.

No trabalho de (DEVICI, 2007, pag. 77) é mencionada a *Bomba-E*, o autor destaca a arma como uma tecnologia de energia direcionada com alto poder de destruição. A bomba eletromagnética é composta por um gerador de pulsos de alta potência, capazes de danificar equipamentos eletrônicos dentro do seu raio de efetividade, como os radares, sistemas de comunicação e navegação. É um dispositivo projetado para destruir equipamentos eletrônicos em um determinado raio de distância. As Bombas-E produzem ondas estacionárias de alta tensão em condutores elétricos ou podem causar explosões eletromagnéticas no nível de gigahertz por meio de radiação, forte o suficiente para derreter o circuito elétrico.

O princípio básico de uma *Bomba E* consiste no uso de um fluxo magnético intenso fornecido pelo gerador da bomba. Empregam-se circuitos magnéticos e bobinas energizadas por um banco de capacitores e essa energia resultante é direcionada através de uma antena. A Figura 5.10 mostra o gerador de compressão que fornece gigawatts de energia para o oscilador que produz as microondas de alta potência.

Figura 5.18- Exemplo de bomba eletromagnética



Fonte: (DEVICI, 2007, pag.77)

As armas de energia direcionada podem proporcionar mudanças nas doutrinas, táticas e estratégias de guerra existentes na atualidade. Assim como os outros sistemas de ataque eletrônico, as principais limitações e desvantagens são:

- A possibilidade de se criar novas tecnologias que restrinjam a eficácia das armas de ED, como contramedidas simples baseadas em pontos negligenciados pelo projeto inicial da arma de ED.
- Algumas armas de ED não são discriminatórias. Além do alvo, qualquer coisa no caminho percorrido pelo feixe poder ser atingida.
- As armas de ED são susceptíveis á degradação pela atmosfera quando há a presença de poeira, nuvens, chuva, fumaça.
- Uma potencial limitação é a avaliação de danos quando se atinge o alvo. A observação direta do efeito causado pode ser complexa.

6. AERONAVES DE ATAQUE ELETRÔNICO

A superioridade aérea no estágio inicial da guerra é considerada uma das chaves para o sucesso na guerra moderna. Baseando-se nessa doutrina, uma aeronave de combate deve ter um alto grau de sobrevivência em um ambiente hostil criado pelo homem.

Para dirimir algumas dúvidas sobre as aeronaves de GE, entende-se que há dois tipos: aeronaves com equipamentos são destinadas para auto-defesa e aeronaves de GE, que são destinadas exclusivamente para emprego nas Ações de Guerra Eletrônica (AçGE) de MAGE e MAE, que será o foco deste capítulo, representada pelas aeronaves empregadas na Marinha (*U.S. Navy*), Força Aérea (*U.S. Air Force*) e Corpo de Fuzileiros Navais *(U.S. Marine Corps)* dos Estados Unidos da América.

Baseado em um Relatório sobre aeronaves de Ataque Eletrônico dos Estados Unidos (USAF, 2016), abordar-se-á as seguintes estadunidenses: EA-18G Growler da U.S Navy’s, EA-6B Prowler do Corpo de Fuzileiros Navais, EC-130H da Força Aérea, F-16CM Block 50 “Wild Weasel.”

6.1 Aeronave EA-18G Growler

O Boeing EA-18G Growler, oferece as principais capacidades de Ataque Eletrônico (EA) e supressão das defesas aéreas inimigas (*SEAD - Sppression of Enemy*

Air Defenses) utilizadas pela U.S Navy's. A aeronave possui uma vasta gama de sensores e armas, seu sistema de armas de sobrevivência pode combater as ameaças atuais e emergentes.

Figura 6.1- EA-18G Growler

Fonte: www.navair.navy.mil/index.cfm?fuseaction=home.display&key=33BFA969-0482-42CF-9E1F-F80A1B32BEE9 (2018)

Conforme é mencionado no relatório, os Estados Unidos possuem quinze esquadrões de Growler EA-18G. Os esquadrões normalmente estão a bordo de dez porta-aviões da U.S Navy's, podendo desempenhar funções nos esquadrões do Corpo de Fuzileiros Navais dos EUA (USMC).

A primeira versão do EA-18G foi a *Block 1*, aeronaves de teste que já saíram de operação. O EA-18G *Block 1* é equipado com até três pods AN/ALQ-99 capazes de bloquear radares inimigos, junto com um receptor AN /ALQ-218 (V) e um sistema para contramedidas em comunicação Raytheon AN / ALQ-227.Os receptores AN / ALQ-99 são instalados na cauda da aeronave e o pod de AN / ALQ-99 abriga os transmissores de interferência de alta potência irradiada.

A principal versão do EA-18G Growler, entrou em serviço em 2010 e consiste na atualização da *Block 1*. Os Growlers que operam atualmente são o *Block 2*. Essa versão é equipada com o radar multimodo AN / APG-79 com modo de detecção passiva

e supressão ativa de radar, receptor de advertência de radar digital ALQ-218 (V) 2 e o ALE-47. Segue abaixo uma breve descrição desses equipamentos.

6.1.1 AN/ALQ-99

O AN/ALQ-99 é um pod capaz de efetuar bloqueio e interceptar automaticamente os radares de vigilância aérea, realiza a aquisição e o rastreamento de sinais desses radares. O pod gerencia os transmissores do sistema para bloquear um grande número de ameaças de radares com energia irradiada efetiva (ERP) muito alta. O AN/ALQ-99 possui uma turbina de ar *Ram* (RAT - ram air turbine) acionada por uma unidade (UEU - universal exciter) e dois transmissores. O UEU gera o sinal de interferência apropriado baseando-se em uma análise computacional e emite o sinal de interferência por meio de dois transmissores de 2 kW e duas antenas de alto ganho. O ALQ-99 possui vários modos de interferência por *spot noise*, e pode ser operado em modos semi-automáticos ou manuais.

Figura 6.2 - AN/ALQ-99 Tactical Jamming System (TJS)

Fonte: www.intelligent-aerospace.com/wrappers/articles-test/2014/03/ai-cobham-antennas.html (2018)

6.1.2 ALQ-218

O ALQ-218 é o grande diferencial da atualização do EA-6B Prowler, a ICAP III (GOODMAN, 2008). O equipamento se trata de um receptor de banda larga, cujo desenvolvimento foi iniciado para resolver deficiências de capacidade contra radares móveis de defesa aérea "pop-up". O ALQ-218 foi produzido pela *Northrop Grumman* e

é considerado um dos primeiros sistemas receptores com essa aplicação que podem executar o bloqueio "seletivo-reativo", ou seja, ele concentra a energia dos pods de interferência ALQ-99 em múltiplas frequências específicas de radar. As tecnologias anteriores trabalhavam bloqueando em larguras de banda maiores, o que pode espalhar a potência de interferência da aeronave durante um ataque eletrônico.

Portanto, o ALQ-218 torna a interferência do Prowler mais precisa. Ele possui a capacidade de identificar com rapidez e precisão a localização de um radar inimigo, detectando-o e aperfeiçoa a região de interferência. Na versão anterior do Prowler, *ICAP II*, seu receptor ALQ-99, fornece a localização aproximada do emissor.

6.1.3 ALQ-227

O ALQ-227 substituiu o jammer de comunicações USQ-113 do Prowler. Esse sistema consiste em um conjunto de contramedidas de comunicações desenvolvido pela *Raytbeon* e que é utilizado no EA-18G. O ALQ-227 é apenas um receptor e não um receptor e jammer como o USQ-113, porém utiliza um pod com curta largura de banda para efetuar o bloqueio em sistemas de comunicação. (GOODMAN, 2008).

6.1.4 Perspectivas de desenvolvimento do EA-18G

A U.S Navy's trabalha para substituir o atual pod ALQ-99 por uma nova concepção de dispositivos de bloqueio, o *Next Generation Jammer (NGJ)*. O NGJ é considerado o próximo passo na evolução do ataque eletrônico aéreo (AEA). Segundo alguns especialistas militares, (GOODMAN, 2008):

> "...o NGJ é necessário para atender às atuais e emergentes lacunas existentes na GE, garantir um sistema unificado capaz de atuar contra as crescentes ameaças e acompanhar os avanços nos sistemas de armas inimigos de forma que haja expansão contínua nas áreas de AEA".

O NGJ será adaptado por meio de um pod sob a fuselagem do Growler. Além disso, esse novo sistema é descrito como um programa de aquisição evolutiva onde o sistema fornecerá capacidade em três componentes incrementais: Incremento 1 (Banda Média), Incremento 2 (Banda Baixa) e Incremento 3 (Banda Alta). A ordem de

desenvolvimento: média, baixa e alta é selecionada conforme a ameaça e pela capacidade de GE disponível na aeronave (USAF, 2016). A Marinha planejou um primeiro teste de um pod totalmente funcional
de Incremento 1 para março de 2019, com previsão de operar em junho de 2021.

Outra abordagem sobre o NGJ (M. Thomas Davis, David Barno and Nora Bensahel, 2014) declara que o *Next Generation Jammer* visa produzir um jammer mais confiável que o ALQ-99 que seria capaz de: interferir em várias bandas e frequências de radares com potência efetiva irradiada (ERP) muito maior e, atinja um número maior de alvos.

Em abril de 2016, a Marinha concedeu à Raytheon um contrato único de US $ 1 bilhão para o Incremento 1, o custo projetado é estimado em US$ 7 bilhões. Em suma, o desenvolvimento do EA-18G e o desenvolvimento final e integração do NGJ custará cerca de US $ 20 bilhões - uma soma significativa, mas menos de 5% do total de custos da aquisição total de caças F-22 e F-35 de quinta geração.

Por fim, os Estados Unidos detêm no programa de desenvolvimento do EA-18G, as melhorias em dispositivos de Ataque Eletrônico das aeronaves através do *Jamming Techniques Optimization (JATO)*, que são atualizações de software e testes relacionados aos equipamentos voltados a GE.

6.2 Aeronaves EA-6B Prowler

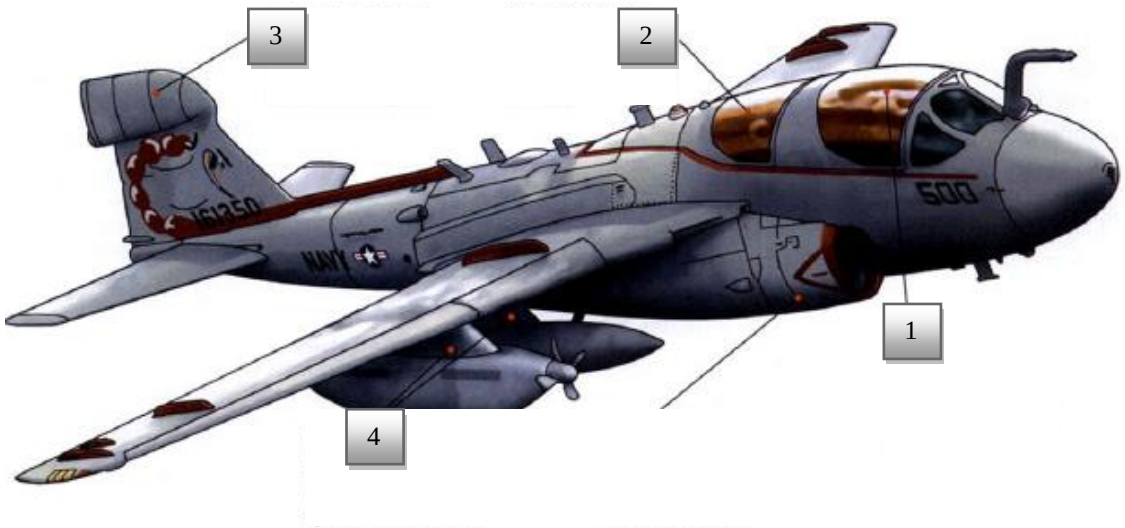
O EA-6B Prowler foi a primeira aeronave da U.S Navy’s dedicada as AçGE e caracteriza-se por possuir avançada capacidade de ataque eletrônico. A aeronave tornou-se operacional em 1971 e foi modernizada várias vezes pela *Northrop Grumman,*. A grande maioria dos EA-6B fazem parte da configuração ICAP II (uma evolução da ICAP I). Embora tenha sido introduzido em 1984, o ICAP II ainda é eficaz para realizar técnicas de bloqueio em radares de defesa aérea e sistemas de comunicação (GOODMAN, 2008).

Figura 6.3- - EA-6B Prowler

Fonte: http://www.mcmahanphoto.com/ny252.html (2018)

O EA-6B transporta um piloto, um oficial de MAE (*Electronic Eounteimeasures Officer* - *ECMO*) sentado ao lado do piloto e mais dois *ECMO* posicionados lado a lado atrás da cabina frontal. A Figura 6.4 detalha algumas partes da aeronave (SCHUSTER, 2010).

Figura 6.4 – Detalhes de MAE do EA-6B Prowler



Fonte: http://www.ea6bprowler.org/ (2018)

1. Cabine do piloto e do oficial de MAE - possui sistemas de navegação, comunicações e MAE.

2. Cabine dos dois operadores dos sistemas de MAE – realiza os controles de bloqueio e apresenta as interfaces gráficas para operação do sistema.
3. Radar Busters – possui um conjunto de antenas na cauda que detecta emissões de radares hostis.
4. Compartimentos adicionais – pode transportar *pods* para realizar bloqueio ou até mesmo mísseis anti-radiação.

Os sistemas de armas EA-6B incluem o ALQ-218, o *pod* de bloqueio ALQ-99, o USQ-113 para realizar MAE COM e o míssil anti-radiação de alta velocidade AGM-88 (USAF, 2016). A seção seguinte detalha brevemente o AGM-88.

6.2.1- Míssil anti-radiação de alta velocidade (HARM) AGM-88

O AGM-88 é um míssil utilizado durante táticas *Standoff* para realizar a supressão letal de defesas aéreas inimigas por aeronaves da U.S Navy's e da Força Aérea americana desde 1984 (PARSONS, 2014). O AGM-88 foi projetado para localizar e destruir radares atrelados a mísseis superfície-ar, radares de alerta antecipado e sistemas de artilharia antiaéreos direcionados por radar, para permitir sobrevôos seguros das aeronaves americanas e aliadas em campo de batalha nas zonas de conflito. O míssil identifica e processa as transmissões emitidas por plataformas contendo radares. (GOODMAN, 2010)

Figura 6.5 - Míssil Anti-Radiação de Alta Velocidade (HARM) AGM-88

Fonte: (https://www.meshfactory.com/agm-88-harm)

O relatório (USAF, 2016) menciona que em 1971 houve a entrega das 12 primeiras aeronaves da produção e que em 1991 ocorreu a entrega dos últimos Prowlers, completando 170 aeronaves entregues. Desde então, os Prowlers foram encarregados pelas missões táticas de GE para a U.S Navy's e para a Força Aérea dos EUA, tendo vasta aplicação desde o início dos anos 90 até a aquisição do EA-18G Growler.

Como foi mencionada acima, a esquadrilha de EA-6B Prowler da U.S Navy's passou por uma série de modernizações na sua capacidade de combate, sendo a mais recente a ICAP III. Os esquadrões do Corpo de Fuzileiros Navais dos EUA recebram sua primeira aeronave ICAP III em 2010. Na U.S Navy's o Prowler teve seu ultimo vôo em 201, sendo substituído pelo EA-18G Growler. O Corpo de Fuzileiros Navais manterá todos os 20 Prowlers restantes até 2019.

No documento embasado para escrever este capítulo cita-se o Sistemas de ataque eletrônico Aerotransportado (AEA). Sistemas que exigem manutenção e atualizações periódicas para ficar à frente das capacidades de guerra eletrônica desenvolvidas ou emergentes de outros países. A U.S Navy's utiliza o AEA para manter o sistema de bloqueio ALQ-99 usado pelo Prowler para garantir a disponibilidade contínua do sistema até que o a próxima geração de *Jammers* atinja a capacidade operacional total (Full Operational Capability - FOC). As aquisições do sistema AEA e os esforços relacionados são necessários para combater as tecnologias modernas e os sistemas emergentes de GE.

Por fim, é relatado que a guerra eletrônica engloba uma série de sistemas inter-relacionados, sendo assim para a eficiência em combate, as modernizaçõess devem ser compatíveis com a esquadrilha. O desenvolvimento de equipamentos de sobrevivência de aeronaves (Aircraft Survivability Equipment - ASE) e contramedidas para as aeronaves da U.S Navy's e Corpo de Fuzileiros Navais envolve estudos e avaliações de ameaças futuras bem como de aeronaves atuais. As modelagens e simulações desse novo ambiente da guerra moderna são importantes para desenvolver tecnologias que aumentem a capacidade de ataque eletrônico da Força.

6.3- Aeronave EC-130H Compass Call

O EC-130H é uma aeronave da U.S Air Force é uma versão modificada do *C-130 Hercules* (projetado para ser uma plataforma de ataque eletrônico em comunicações aéreas). O EC-130H teve como principal missão realizar as funções de bloqueio e despistamento em radares de defesa aérea inimigos.

Figura 6.6 - EC-130H Compass Call

Fonte: www.radarphotography.com/thunder---lightning-over-arizona-2016.html (2018)

O sistema de MAE presente nesta aeronave degrada as comunicações de comando e controle (C2) do inimigo e reduz a capacidade de coordenação em combate da vítima. O sistema *Compass Call* utiliza contra-informação ofensiva e capacidade de ataque eletrônico (EA) em apoio às forças aéreas e de superfície. O relatório (USAF, 2016) menciona que o EC-130H, o EA-6B ou o EA-18G e o F-16CM formam o que é chamado de “trio SEAD”, uma vez que operam em em conjunto para derrotar os sistemas de defesa aérea adversários. As modernizações realizadas de forma planejada aumentaram a robustez da aeronave e ela veio a adquirir recursos secundários de ataque eletrônico contra os radares de aviso antecipado e de aquisição.

O EC-130H pode transportar até treze militares, sendo que nove desses militares operam os equipamentos de Ataque Eletrônico. A tripulação inclui o comandante da tripulação de GE, oficial de sistema de armas, supervisor de GE, quatro operadores para análise de dados, “um operador de aquisição” e um técnico de manutenção aerotransportada, ou seja, militares preparados para exercer as funções específicas

durante uma missão de GE no ar. A aeronave possui antenas, recebendo sinais de radiofrequência que são analisados por uma equipe de aviadores que tomam uma decisão sobre como afetar o espaço de batalha inimigo baseado nos sinais recebido, em um espectro de RF.

Figura 6.7 - EC-130H possui antenas (sob a fuselagem),

Fonte: https://www.military.com/dodbuzz/2017/07/25/airmen-fighting-isis-talk-future-electronic-attack-aircraft-ec-x

A esquadrilha de 14 aviões EC-130H é composta por duas versões de aeronaves: Linhas de base 1 e 2. A primeira aeronave da linha de base 2 foi recebida em 2014, na Base Aérea Davis-Monthan (AFB), Arizona.

6.3.1 Primeira versão do EC-130H

Essa primeira versão ficou conhecida como Linha de Base 1 do EC-130H e apresenta recursos para bloquear: comunicações, radares de aviso antecipados, radares de vigilância aérea e sistemas de navegação. Utilizam-se técnicas de alta potencia irradiada, larga faixa de frequência e processamento digital de sinais.

6.3.2 Segunda versão do EC-130H

A segunda versão proposta pela Linha de Base 2 trouxe várias atualizações para otimizar o trabalho de quem opera a aeronave e tornar todo o sistema mais eficiente. A Força Aérea americana informa que foi introduzido a essa versão o gerenciamento automatizado de recursos. As melhorias nas comunicações externas permitiram que as equipes do EC-130H mantenham a consciência situacional e a conectividade em ambientes operacionais dinâmicos. As melhorias encontradas na Linha de Base 2 do EC-130H são modificações que aumentam a precisão e a capacidade de ataque eletrônico. Os recursos de comunicação das aeronaves foram aprimorados com a expansão da conectividade de comunicações via satélite, compatível com as arquiteturas emergentes. Por fim, as modificações na estrutura proporcionaram melhor desempenho e capacidade de sobrevivência das aeronaves.

6.4 F-16CM Block 50 “Wild Weasel.”

O *Block 50* é uma das versões do F-16 que a Força Aérea americana possui em seu vasto arsenal e passou a ser utilizada para testes operacionais em 1991. A modernização realizada trouxe um aprimoramento na sua propulsão, melhorando o desempenho da aeronave. No ano de 1993, foram introduzidas novas mudanças para as missões de GE, sendo inseridos mísseis Anti-Radiação *AGM-88 HARM* **(***High-Speed Antiradiation Missile)* que operam por meio do *Pod ASQ-213 HTS (HARM Targeting System).*

Figura 6.8 - F-16CM Block 50

Fonte: https://militaryaiworks.com (2018)

O *HTS* possui um sistema temido pelas forças inimigas uma vez que pode contribuir para a supressão da defesa aérea da vítima. Este sistema proporciona aos pilotos uma consciência situacional sobre os tipos e locais dos radares de defesa terra-ar, e também interage com o míssil HARM sempre que o mesmo é lançado. O sistema melhora a precisão do míssil anti-radiação AGM-88 HARM, fornecendo a distância e direção dos radares de defesa aérea inimigos.

Figura 6.9 – Pod ASQ-213 instalado no F-16CM Block 50

Fonte: www.tapatalk.com (2018)

Os F-16 equipados com HTS geralmente operam em conjunto com aeronaves de reconhecimento eletrônico Air Force RC-135 Rivet Joint e aeronaves de guerra eletrônica EA-6B Prowler. O Block 50 foi desenvolvido para fornecer um avanço significativo na tecnologia de ataque eletrônico e preencher o vazio deixado pela aposentadoria do *F-4G Wild Weasel*. O primeiro esquadrão de F-16CM Block 50 entrou em operação em 1994, a Força Aérea continuou a comprar quantidades adicionais de pods HTS e agora planeja adquirir estes dispositivos de MAE para equipar toda a frota do Bloco F-16 50/52 (USAF, 2016). O capítulo seguinte realizará uma abordagem do emprego tático de algumas aeronaves de ataque eletrônico, descrevendo alguns acontecimentos verídicos ocorridos em conflitos empregando GE.

7- EMPREGO TÁTICO DAS AERONAVES DE MAE

O emprego da Guerra Eletrônica vem ocorrendo nas operações militares desde os primórdios do radar e a evolução contínua nas tecnologias contribuiu para isso, progressos como: materiais semicondutores, hardwares com maior poder de processamento e técnicas inovadoras utilizadas pelos equipamentos embutidos no cenário da guerra moderna. Isso tudo vem ocorrendo graças à grande contribuição de engenheiros, cientistas e militares que detém conhecimentos de táticas de guerra.

Para contextualizar o assunto referente ao capítulo é necessário relembrar alguns acontecimentos ocorridos durante a Segunda Guerra Mundial, principalmente na perspectiva americana. Naquela época, os radares de alerta antecipados posicionados em terra foram usados durante conflitos para detectar aeronaves inimigas a longas distâncias. Estes radares de superfície aumentavam significativamente as chances de sucesso das defesas aéreas, uma vez que se comunicavam com as artilharias antiaéreas para realizar a interceptação das aeronaves inimigas. Diante desse cenário os Aliados e a Alemanha desenvolveram rapidamente uma série de contramedidas para negar ou degradar estes radares. O Chaff foi desenvolvido e usado pelos Aliados e pela Alemanha para despistar ou bloquear os radares de vigilância aérea. Eles também realizaram bloqueios em radares e modificaram suas táticas aéreas para reduzir o tempo de exposição da aeronave dentro da cobertura de radares inimigos. (USAF, 2016)

Assim como as contramedidas foram desenvolvidas para combater radares, também foram desenvolvidas contra as próprias contramedidas anti-radar. Nesse cenário, a Alemanha começou a usar frequências de radar que não foram afetadas pelos Chaff aliados. Os alemães desenvolveram novas técnicas de interceptação das transmissões dos radares de navegação de aeronaves. Eles também conseguiram identificar aeronaves por meio de radares Doppler cujo eco recebido carregava características da hélice da aeronave identificada.

As pesquisas e o desenvolvimento em radares resultaram em um ambiente de guerra onde o radar passou a fornecer informações precisas para guiar mísseis até o alvo. Em contraposição, os Estados Unidos procuraram aumentar a capacidade de sobrevivência das aeronaves de várias maneiras.

Algumas aeronaves, como a U-2, voavam em altas altitudes. As aeronaves SR-71 voavam em altas altitudes e em altas velocidades. Os F-111 voavam muito rápidos e em baixas altitudes. Além disso, muitas dessas aeronaves já detinham sistemas de contramedidas eletrônicas.

Figura 7.1 - Aeronave F-111

Fonte: https://www.pinterest. (2018)

Perante a crescente evolução nos sistemas de armas, durante a Guerra do Vietnã, os Estados Unidos desenvolveram muitas técnicas para melhorar a capacidade de sobrevivência das aeronaves contra as defesas aéreas integradas do Vietnã do Norte. Os americanos possuíam:

- aeronaves SEAD F-105 “Wilde Weasel”
- mísseis anti-radiação
- plataformas aerotransportadas de bloqueio, como o EA-6B Prowler e o EF-111 Raven.

O aumento no alcance de mísseis de superfície que eram lançados no ar, *SAMs - surface-to-air missiles*, e as melhorias nos radares de superfície também induziram o avanço na capacidade de sobrevivência das aeronaves. Os F-117 Night Hawk (Figura 5.2) eram aeronaves que utilizavam novos materiais e técnicas para reduzir emanações de calor e para desviar ou absorver emissões de radares, os F-117 reduziram significativamente a probabilidade de detecção e rastreamento pelo inimigo. Mesmo diante de toda essa tecnologia, a derrubada de uma dessas aeronaves (antes considerado invisível ao radar) no conflito de 1999 na Iugoslávia por um SAM sérvio, ilustra que o

controle do espectro eletromagnético é um esforço contínuo para as forças aéreas de todo o mundo.

Figura 7.2 - *F-117 Night Hawk* e ao lado os destroços do modelo derrubado em combate

Fonte: www.cavok.com.br e www.military-today.com (2018)

7.1 - MAE na Guerra Aérea contra o Vietnã do Norte

Em um relatório sobre táticas e técnicas de Guerra Eletrônica da Força Aérea americana foi apresentado detalhadamente as missões envolvendo medidas de ataque eletrônico no ar, durante a Guerra do Vietnã (NALTY, 1977). No documento é abordado que a Força Aérea utilizou as aeronaves EB-66B e EB-66C em missões de GE contra os norte – vietnamitas, elas eram empregadas normalmente durante missões de Standoff Jamming. Os EB-66 detectavam e coletavam informações sobre locais e frequências de radares inimigos, combatendo as defesas antiaéreas e os mísseis superfície-ar (SAMs). Os EB-66 carregavam dispositivos para realizar bloqueio por meio de nove transmissores (na versão EB-66C) e possuíam vários dispositivos para lançamento de Chaff.

Figura 7.3 – Aeronave de ataque eletrônico EB- 66

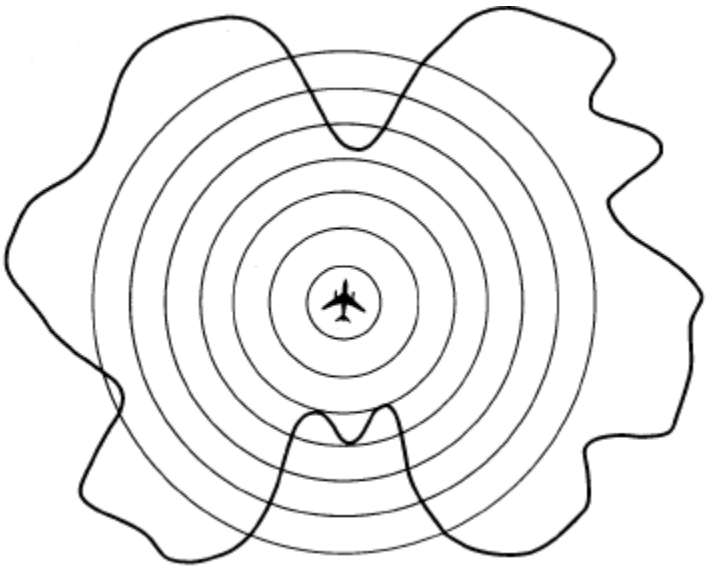
Fonte: www.nationalmuseum.af.mil (2018)

Naquela época, durante uma das missões, dois EB-66C decolaram de *Takhli*, e completaram seus tanques de combustível através de uma aeronave *Stratotanker* Boeing KC-135, e se juntaram com a força aérea de ataque. Conforme o relatório, as duas aeronaves acompanharam os caças-bombardeiros até a vizinhança do alvo, depois entraram em uma órbita elíptica entre 25.000 e 30.000 pés, além do alcance de armas antiaéreas de 37 mm ou 57 mm. Os oficiais de GE bloquearam os radares *Fire Can* (radares de vigilância aérea), enquanto monitoravam os sinais da *Fan Song* (denotação utilizada para radares de vigilância e controle de armas). Se a equipe recebesse a duplicação da frequência de repetição de pulsos (FRP) do *Fan Song* ou do sinal de orientação do SAM, o oficial chefe de GE alertava a força aérea de ataque pelo rádio e tomava as devidas medidas de ataque eletrônico para bloquear o feixe de rastreamento do *Fan Song*.

Os EB-66B fizeram sua estréia no combate em outubro de 1965 e logo demonstraram que o poder de interferência que lhes permitia fechar com o alvo também poderia ser uma defesa. O ruído eletrônico proveniente do avião interferia com seu equipamento de alerta de radares. Como resultado, o EB-66B e o EB-66C tiveram que trabalhar juntos. Os EB-66B utilizavam técnicas de bloqueio por Ruído de barragem (cobria as frequências que o inimigo estava usando) com faixa frequência mais ampla e sinais mais fortes, proporcionando melhor proteção contra os SAMs e permitindo que os modelos EB-66C permanecessem bem além do alcance de 17 milhas náuticas do alcance útil dos mísseis inimigos e fornecendo aviso de SAM.

Outro fato interessante foi que os oficiais que planejaram as missões de interceptação do EB-66 tiveram que levar em conta o fato de que o ruído gerado por essas aeronaves não irradiava das antenas em um padrão uniforme e concêntrico. A localização da antena fez com que a cobertura de bloqueio se parecesse com uma espécie de borboleta, o avião no centro e os sinais mais fortes irradiando perpendicularmente à trajetória de vôo. Dessa forma, a tática era atribuir os aviões em pares, organizando a órbita de modo que um deles estivesse sempre ao lado do radar inimigo.

Figura 7.4 – Padrão de radiação do bloqueio da aeronave EB-66



Fonte: NALTY (1977)

7.2- Aplicações do EA-6B Prowler

Durante os últimos anos, tornou-se comum ter quatro ou cinco esquadrões da U.S. Navy e do Corpo de Fuzileiros Navais enviados ao Comando Central dos EUA (CENTCOM) área de responsabilidade (AOR), operando ao mesmo tempo em terra ou no ar, no Iraque ou no Afeganistão. A U.S. Navy e os fuzileiros navais têm voado seus EA-6Bs em taxas de utilização recorde em apoio a operações contra o terrorismo e operações no Iraque (*Operation Enduring Freedom- OEF* e *Operation Iraqi Freedom- OIF).* Segundo o relatório (GOODMAN, 2008), as missões EA-6B no Iraque e no Afeganistão envolveram o apoio a forças do Exército e da U.S Navy's realizando bloqueio nos sistemas de comunicação inimigos, particularmente durante vôos para

neutralizar os dispositivos de ativação de explosivos implantados de forma improvisada por rebeldes da região.

7.3- Aplicações do EC-130

A missão do EC-130 é "negar do céu", o que significa frustrar a capacidade de um adversário de conduzir comunicações de comando e controle. Embora isso geralmente signifique interromper outros sistemas de armas. Os Estados Unidos utiliza essa aeronave na luta contra o Estado Islâmico do Iraque e do Levante (ISIS), grupo considerado uma organização terrorista estrangeira. O EC-130 permite interferir nas comunicações de rádio no solo. Conforme Joshua (2017), o ISIS é bem treinado e eficaz em seu método de guerra. Por meio da aeronave é possível usar contra-táticas, em uma espécie de jogo de “gato e rato” à medida que avançam suas técnicas. A plataforma de ataque eletrônico irá monitorar o ambiente de alcance e ao receber um sinal e explorá-lo, sinais específicos são direcionados em um espectro de frequência de rádio.

Por se tratar de uma tecnologia empregada na guerra moderna pelos americanos, nota-se que os detalhes de funcionamento dos equipamentos de ataque eletrônico dessas aeronaves nem sempre são descritos de forma concisa, uma vez que o sigilo dos detentores da tecnologia pode resultar no sucesso da missão empregando a tecnologia.

8. CONCLUSÃO

O trabalho abordou os principais tipos de Medidas de Ataque Eletrônico (MAE) usadas em missões de GE envolvendo aeronaves. O foco do estudo foi dado nas MAE não destrutivas incluindo técnicas de bloqueio e despistamento e abordou de forma menos detalhada as MAE destrutivas. As táticas de ataque eletrônico (AE) mais usadas em combates aéreos foram descritas para compreender a forma pela qual essas aeronaves utilizam os dispositivos de AE. Alguns dos equipamentos embarcados em aeronaves de MAE foram mencionados e descritos de forma a demonstrar o poder de combate que esses dispositivos possuem. O emprego tático dessas aeronaves pôde ser constatado no ultimo capítulo do trabalho, ao descrever algumas aplicações reais dessas aeronaves em conflitos que ocorreram há aproximadamente cinco décadas e também em missões de GE que ocorrem atualmente.

Foi possível verificar que as tecnologias de Guerra Eletrônica usadas em aeronaves estão se desenvolvendo cada vez mais. Além disso, nota-se que a sobrevivência das aeronaves na guerra moderna dependerá da capacidade de ganhar superioridade na GE. Portanto, assim como os países desenvolvidos, a Marinha do Brasil deve se atualizar e buscar a modernização de seus meios no que se refere à MAE nas aeronaves. O desenvolvimento só será possível por meio de investimentos em novos meios, em inovações tecnológicas, treinamento de pessoal e um programa doutrinário indispensáveis para inserir-se com sucesso em futuros ambientes de combate.

Foi realizada uma revisão bibliográfica envolvendo conceitos de MAE, os tipos de MAE e as diferentes abordagens feitas pelos autores. Por meio de artigos, relatórios e outros documentos foi possível abordar alguns dispositivos de AE e as principais aeronaves de MAE. Isso tudo contribuiu para o arcabouço de conhecimento referente ao tema apresentado.

8.1 Considerações Finais

Em países como os Estados Unidos o domínio na área de GE durante os últimos 25 anos é indiscutível. No entanto, a diferença existente entre os Estados Unidos e os países emergentes vem diminuindo consideravelmente nos últimos anos por motivos já mencionados no trabalho. Assim como esses países que deram um grande salto e estão avançados no desenvolvimento de tecnologias de GE em aeronaves, a Marinha do Brasil precisa almejar sempre um novo patamar na GE, para que suas aeronaves consigam sobreviver e cumprir futuras missões utilizando AE.

8.2 Sugestões para Futuros Trabalhos

O trabalho realizou uma abordagem geral das aeronaves de AE e um passo que pode ser dado é viabilizar a implementação de algumas tecnologias de AE nas aeronaves da Marinha do Brasil. Por meio do levantamento das características atuais das aeronaves existentes na Força Aeronaval, buscando possíveis modernizações nos sistemas de GE. Os americanos mostraram que economicamente é mais viável o investimento na modernização de antigas aeronaves que a compra de aeronaves novas de GE.

O embasamento teórico utilizado neste documento, durante algumas abordagens, empregou material da Força Aérea dos Estados Unidos (USAF) e da Força Aérea Brasileira (FAB). Faz-se necessária uma abordagem fundamentada em referências que contenham descrições tanto técnicas e táticas quanto doutrinárias voltadas para a Marinha. A título de continuidade do trabalho, pode-se focar na U.S. Navy de forma a servir como arcabouço teórico, bem como buscar referências de outras Marinhas que detém conhecimento do tema proposto.

REFERÊNCIAS

BARNO, D.; BENSAHEL N.; DAVES T. **The Enduring Need for Electronic Attack in Air Operations.** *Policy Brief.* Jan, 2014.

DAVIS M. T.; BARNO D; BENSAHEL N. The Enduring Need for Electronic Attack in Air Operations. **Center for a New American Security,** Washington, 2014.

DEVECI; B. M. **Directed-Energy Weapons: Invisible And Invincible?.** Naval Postgraduate School. Sep, 2007.

EMA 305, **Doutrina Militar Naval.** Marinha do Brasil, Estado-Maior da Armada, 2017.

GOODMAN, G. **Prowler to Growler: Divergent Paths**. T*he Journal of Electronic Defense*, May, 2008, Vol.31(5), p.36(7).

GOODMAN, G. **The New Face of Airborne Electronic Attack**. *The Journal of Electronic Defense*, April, 2010, Vol.33(4), p.28(6)

HAYSTEAD, J. **US Helicopter EW.** ***Journal of Electronic Defense***. 35, 3, 26-35, Mar. 2012. ISSN: 0192429X.

JOSHUA < https://www.military.com/dodbuzz/2017/07/25/airmen-fighting-isis-talk-future-electronic-attack-aircraft-ec-x> Acesso em: 10 de maio de 2018

KELLER, J. **Helicopter-based electronic warfare to protect ships from missiles**. *Military & Aerospace Electronics*. 28, 2, 27, Feb. 2017. ISSN: 10469079.

Ministério da Defesa. Comando da Aeronáutica - FAB. **Guerra Eletrônica**, *Medidas de Ataque Eletrônico*. Brasília, DF, 2011.

NALTY B C. **THE AIR FORCE IN SOUTH EAST ASIA.** *Tactics And Techniques Of Electronic Warfare*, Aug., 1977.

NERI, F. **Introduction to Electronic Defense Systems.** 2.ed. U.S.A: SciTech Publishing Inc. Raleigh. NC, 2006.

PARSONS, D**. Improved HARM bang on target in weapons test.** *Flight International,* Vol:186 Fasc:5454 p.:16, 2014.

QUARANTA, P. **Airborne Electronic Warfare. (Cover story).** *Military Technology*. 32, 4, 110-121, Apr. 2008. ISSN: 07223226.

QUARANTA, P. **Airborne Electronic Warfare Today and Tomorrow.** *Military Technology*. 39, 6, 54-56, June 2015. ISSN: 07223226.

SANTOS A. Pod sky-shield - Aliado indispensável da caça no cenário de guerra moderna. **Spectrum – Revista do Comando-Geral de Operações Aéreas**, n.12, p. 4-6, 2009.

SCHUSTER, C. O. **The EA-6B Prowler: outwitting Hanoi's Air Defenses.(ARSENAL).** *Cengage Learning, Inc. Vietnam*, April, 2010, Vol.22(6), p.15(1).

USAF, Congressional Research Service **U.S. Electronic Attack Aircraft,** 2006.

USAF, United States Air Force. **Electronic Warfare Fundamentals**. U.S.A, 2000.

USAF, United States Air Force. **U.S. Electronic Attack Aircraft**. U.S.A, Jul., 2016.

WILSON, JR. **Electronic warfare evolves to meet new threats: U.S.** Military feels pressure to keep its technological lead in a never-ending battle for the electromagnetic spectrum. *Military & Aerospace Electronics*. 28, 8, 10-19, Aug. 2017. ISSN: 10469079.