RESERVADO

MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
GUERRA ELETRÔNICA

TRABALHO DE CONCLUSÃO DE CURSO

GUERRA ELETRÔNICA DE COMUNICAÇÕES: técnicas de MPE.

1°Ten RENAN DA CUNHA PINTO

Rio de Janeiro
2021

RESERVADO

RESERVADO

1°Ten RENAN DA CUNHA PINTO

GUERRA ELETRÔNICA DE COMUNICAÇÕES: técnicas de MPE.

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

Orientadores:
CT Willian Sathler Lino Soares

CIAW
Rio de Janeiro
2021

RESERVADO

FOLHA DE APROVAÇÃO

1°Ten RENAN DA CUNHA PINTO

GUERRA ELETRÔNICA DE COMUNICAÇÕES: técnicas de MPE.

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:

CT Willian Sathler Lino Soares - CIAW _____

CT Rafael Vieira da Silva – Cv Júlio de Noronha _____

Prof. Dr. Renato Barbosa de Oliveira – PUC-Rio _____

CIAW
Rio de Janeiro
2021

RESERVADO

Dedico esse trabalho àqueles que, de alguma forma, me fizeram parte dos momentos de aprendizado e me ajudaram a me tornar a pessoa que sou hoje.

AGRADECIMENTOS

Agradeço primeiramente a Deus, que guiou meus estudos e caminhos durante esse curso e em toda a minha vida, sendo minha base e minha fortaleza nesse período de árduos estudos.

Agradeço aos meus pais, Roberto Carlos e Selmara, que, com todo o amor, me prestaram todo apoio e auxílio, e, como sempre, cuidaram de todos os detalhes do dia a dia para que pudesse me dedicar exclusivamente ao curso.

A minha namorada e amiga Ana Carolina Martins, que tem acompanhado as minhas dificuldades e vitórias, sendo sempre muito compreensiva e parceira em todas as áreas da minha vida.

Ao Capitão-Tenente Sathler, que muito colaborou com aconselhamentos e direcionamentos como orientador e coordenador, sendo parte fundamental para a minha conclusão nesse curso.

“Não se admitem surpresas para o nauta: há de adivinhar a atmosfera como o barômetro, e pressentir a tormenta, quando ela pinta apenas como uma mosca pequenina e longínqua na transparência da imensidade. O mar é um curso de força e uma escola de previdência. Todos os seus espetáculos são lições: não os contemplemos frivolamente.” – Ruy Barbosa

GUERRA ELETRÔNICA DE COMUNICAÇÕES: técnicas de MPE

Resumo

O mundo está em constante evolução. Ao pararmos para refletir sobre como, tecnologicamente, o mundo era a poucas décadas atrás e como se encontra agora, perceberemos uma diferença acachapante. A evolução tecnológica que presenciamos no século passado, especificamente após a Segunda Guerra Mundial, é aterrorizante. Radares cada vez mais modernos, sistemas de comunicações, sistemas de direção de tiro, sistemas de propulsão cada vez mais modernos e integrados são reflexo diretos dessa assombrosa e colossal evolução. Essa tamanha evolução tem sido grande motivador para alavancar as pesquisas de novas técnicas para a Guerra Eletrônica (GE) e suas medidas: Medidas de Apoio À Guerra Eletrônica (MAGE), Medidas de Ataque Eletrônico (MAE) e as Medidas de Proteção Eletrônica (MPE). As técnicas como Bloqueio Eletrônico, Salto em frequência, Controle de Potência, Antenas Direcionais, Criptografia, Criptofonia, Esteanografia, dentre outras, vem se destacando, evoluindo e se tornando poderosas medidas a serem utilizadas pela Guerra Eletrônica e suas medidas.

Palavras- chave: Guerra Eletrônica. Marinha do Brasil. Comunicações. Medidas de Proteção Eletrônica.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

AGE	Atividades de Guerra Eletrônica
APEL	Aprestamento Eletrônico
BRF	Bloqueio de Rádio Frequência
C2	Comando e Controle
CGE	Capacidade de Guerra Eletrônica
CONSET	Condição de Silêncio Eletrônico
CT&I	Ciência, Tecnologia e Inovação
DBM	Doutrina básica da Marinha
DT	Direção de Tiro
EEM	Espectro Eletromagnético
END	Estratégia Nacional de Defesa
FFAA	Forças Armadas
GE	Guerra Eletrônica
IEEE	Instituto de Engenheiros Eletricista e Eletrônicos
MAE	Medidas de Ataque Eletrônico
MAGE	Medidas de Apoio a Guerra Eletrônica
MB	Marinha do Brasil
MD	Ministério da defesa
MGE	Medidas de Guerra Eletrônica
MPE	Medidas de Proteção Eletrônica
OM	Organizações Militares
RETRON	Reconhecimento Eletrônico
SARP	Sistemas de Aeronaves Remotamente Pilotadas
SNR	Relação Sinal-Ruído

LISTAS DE SÍMBOLOS

Pr	potência recebida;
Pt	potência transmitida;
Gt	ganho da antena transmissora;
Gr	ganho da antena receptora;
λ	comprimento de onda;
π	constante matemática com valor aproximado de 3,1416;
d	distância entre o transmissor e o receptor (em metros);
L_{TOTAL}	perda de propagação (atenuação);
log	logaritmo; e
dB	decibel.

SUMÁRIO

1 INTRODUÇÃO

Ao longo da história do homem, a comunicação sempre teve papel fundamental, tanto no âmbito socioeconômico quanto tecnológico. Meios de comunicações tradicionais, como televisão e rádio, se adequaram as novas tecnologias, fossem estas originadas de necessidades comerciais, civis, ou militares, sendo que esta última está associada à obtenção de vantagens sobre outros países, tanto aliados quanto oponentes.

O avanço da tecnologia tem desenvolvido cada vez mais os equipamentos empregados na Guerra Eletrônica (GE). Podemos encontrar equipamentos cada vez mais sofisticados, os quais trabalham com multiplexação de tarefas ininterruptamente, com maior eficiência e eficácia no processamento de dados, na identificação de emissões. O tempo de realização de atividades tem se reduzido e continua a diminuir cada vez mais, fruto de tal avanço.

Faz-se, então, necessário repensar as Medidas de Proteção Eletrônica (MPE) de modo que não fiquem defasadas devido a essas evoluções. O aumento na capacidade de processamento de dados e automação trouxe, agora, uma enorme responsabilidade ao operador do sistema de comunicações a fim de evitar as ofensivas atuais.

É de suma importância para as Forças Armadas (FFAA) e para a Estratégia Nacional de Defesa (END) que os militares conheçam os recursos de GE disponíveis tanto nos meios que operam, quanto em uma Força quando operando conjuntamente. Por muitas vezes, não se atinge esse objetivo devido à falta de interoperabilidade entre as Forças Armadas.

Tal avanço tecnológico tem possibilitado o emprego de equipamentos cada vez mais modernos nas comunicações, trazendo consigo, um aumento no número de interceptações e ataques. É nesse contexto que se reforça a necessidade de se manterem atualizadas as MPE seja contra o bloqueio de sinais ou a interceptação e alteração de mensagens transmitidas, evitando que sejam comprometidas a integridade, segurança e disponibilidade das comunicações.

As técnicas e procedimentos de MPE ganham destaque quando os equipamentos de comunicação não podem permanecer na Condição de Silêncio Eletrônico (CONSET), ou seja, sem realizar emissões.

Toda vez que um meio emite uma onda eletromagnética com um dos seus equipamentos, surge a oportunidade para o inimigo obter informações, estratégicas e táticas, através das Medidas de Apoio à Guerra Eletrônica (MAGE) e de interferir no trânsito das mesmas por meio de suas Medidas de Ataque Eletrônico (MAE).

Sendo assim, nas operações militares, faz-se necessário o conhecimento das novas tecnologias, dos equipamentos de comunicações e das análises comportamentais de ondas eletromagnéticas, no teatro de operações, a fim de que seja possível, de maneira eficaz, a aplicação de meios e recursos que possibilitem reduzir, anular ou impedir Ações de Guerra Eletrônica (AGE) através das MPE.

1.1 Apresentação do Problema

As comunicações são de suma importância para uma Força Aramada (FA). É através dela que é feito grande parte do tráfego de informações, dos mais variados graus de sigilo, onde os Comandantes e Diretores realizam a coordenação e o controle das Organizações Militares (OM) sob sua liderança, sejam elas prédios, navios, depósitos ou tropas. Para a Marinha do Brasil (MB) não é diferente. Quando um navio ou uma força se faz ao mar, diversas mensagens são trafegadas sejam elas por voz, dados ou links e, junto com elas, inúmeras informações de todo teor as quais, se nas mãos da força inimiga, acarretaria em danos inimagináveis.

No que tange as perspectivas atuais e futuras de emprego das Forças Armadas (FFAA), os desafios a serem enfrentados pela MB, quando consideramos a evolução tecnológica a qual estamos presenciando e a que ainda está por vir, serão de enormes e revestir-se-ão de grande relevância e se fazem necessários métodos eficientes de proteção de suas comunicações.

1.2 Justificativa e Relevância

A Guerra Eletrônica (GE) já saiu da esfera de tecnologia do futuro e se tornou uma realidade mundial. O Brasil está inserido em um cenário onde as grandes potências militares globais, como Estados Unidos, Rússia e China, por exemplo, possuem um vasto conhecimento técnico e tecnológico capazes de provocar uma revolução nessa área. Desse

modo, as emissões eletromagnéticas tendem a passar por transformações em determinados aspectos, tais como a segurança de suas transmissões.

Devido a isso, torna-se de grande relevância a ampliação das capacidades e mentalidade de GE por parte das FFAA brasileiras. Sendo assim, é justificável o estudo de técnicas mais modernas de GE de modo a possibilitar uma melhor compreensão das possibilidades e vulnerabilidades que trarão aos sistemas de comunicação utilizados na MB.

Acrescendo à relevância desse trabalho, deve-se considerar a necessidade de evitar a desatualização dos conhecimentos teóricos e técnicos relativos à GE, uma vez que os estudos e o conhecimento evoluem conforme surgem novas tecnologias e equipamentos. É nesse contexto de constante evolução e atualização que as contramedidas, tais como as Medidas de Proteção Eletrônica, se revestem de grande importância visando à garantia da operabilidade, combatividade e a funcionalidade dos sistemas vitais para as FFAA.

1.3 Objetivos

O objetivo deste trabalho se baseia em apresentar os conceitos de GE e estimular a difusão e o aprofundamento do tema na MB.

1.3.1 Objetivo Geral

Consoante ao exposto na Introdução e Apresentação do Problema, os conceitos da GE são de grande relevância nas comunicações. O objetivo geral deste trabalho se baseia em apresentar os conceitos de GE bem como de técnicas modernas de MPE.

1.3.2 Objetivos Específicos

Este trabalho tem como objetivos específicos apresentar técnicas de Medidas de Proteção Eletrônica e sua aplicação nas comunicações na MB.

1.4 Etapas do Trabalho

Este trabalho foi dividido em 5 capítulos.

Na Introdução, o tema foi exposto e contextualizado, sendo feito apresentadas as motivações e os objetivos deste trabalho.

No Referencial Teórico será realizada a contextualização do tema, uma vez apresentados os seus conceitos básicos.

Na Metodologia abordar-se-ão as classificações da pesquisa, as limitações da metodologia e como foram realizadas as coletas dos dados.

No capítulo Guerra Eletrônica Nas Comunicações serão apresentados exemplos de tecnologias que podem ser utilizadas nas Medidas de Proteção Eletrônica.

Na Conclusão, último capítulo deste trabalho, será apresentado o desfecho desse estudo e propostas para trabalhos posteriores.

2 REFERENCIAL TEÓRICO

2.1 Guerra Eletrônica: Uma Visão Geral

O presente capítulo visa apresentar o conceito da Guerra Eletrônica e suas ramificações. Em linhas gerais, esse trabalho se concentra na subdivisão das Medidas de Proteção Eletrônica (MPE), cujo propósito é permitir o próprio uso do espectro eletromagnético (EEM), que, resumidamente, corresponde a toda faixa de frequências em que um determinado sinal eletromagnético pode se propagar, contra ações de oposição (MAE inimiga) com intuito de impedir e negar o fornecimento de informações por interceptação do sinal eletromagnético pelo inimigo.

O objetivo das Medidas de Ataque Eletrônico é interferir no uso efetivo do espectro eletromagnético pela força inimiga e seu sucesso é atingido quando o sinal interferente impossibilita que o oponente consiga obter os dados e as informações de interesse. Daí, a importância de se adotar Medidas de Proteção Eletrônica, uma vez que é através do EEM que são transmitidas informações que podem ser sob a forma de voz e dados, por exemplo.

Por outro lado, as Medidas de Apoio à Guerra Eletrônica (MAGE) possuem uma natureza passiva e visam, fundamentalmente, a capitação de dados e informações para a identificação e localização de seu emissor de modo que a apoiar o comando para o processo decisório; tais informações serão úteis para avaliação das ameaças e orientação de emprego de MPE em nossos meios e de MAE aplicadas aos sistemas de comunicação do inimigo, possibilitando realizar interferências em seu enlace de comunicações.

2.2 O Conceito de Guerra Eletrônica

Com o decorrer do tempo, a guerra vem se desenvolvendo e evoluindo. O surgimento de novas tecnologias nos apresenta ambientes de guerra que, décadas atrás, não existiam. Nesse contexto de plena evolução tecnológica, ganha cada vez mais relevância a Guerra Eletrônica.

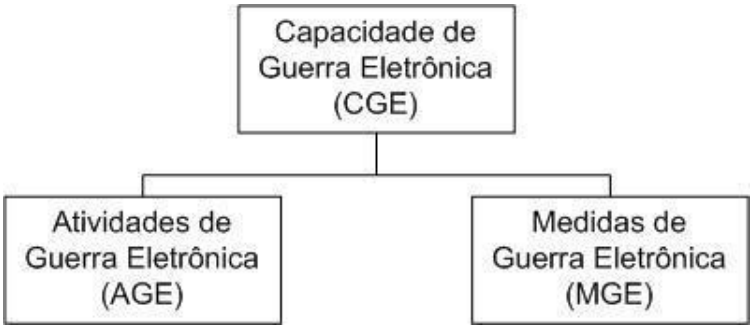
De acordo com a Doutrina Básica da Marinha (DBM) e o Manual de Guerra Eletrônica, o conceito de Guerra Eletrônica é observado como:

> Conjunto de ações que visam a explorar as emissões do inimigo, em toda a faixa do espectro eletromagnético, com a finalidade de conhecer a sua ordem de batalha, intenções e capacidades e, também, utilizar medidas adequadas para negar, reduzir ou prevenir o uso efetivo dos seus sistemas, enquanto se protege

> e utiliza, com eficácia, os seus próprios sistemas (MARINHA DO BRASIL, 2016a).

Suas possibilidades, também conhecida como Capacidade de Guerra Eletrôncia (CGE), é constituída pelo somatório de todos os recursos necessários a uma força para pôr em prática eficazmente as ações de GE. A CGE se fundamenta sob dois grupos: Atividades de Guerra Eletrônica (AGE) e Medidas de Guerra Eletrônica (MGE) conforme apresentado na Figura 1.

Figura 1: Estrutura das Capacidades de Guerra Eletrônica.



Fonte: (MARINHA DO BRASIL, 2016a).

2.2.1 Atividade de Guerra Eletrônica (AGE)

As Atividades de Guerra Eletrônica (AGE) são caracterizadas por possuírem uma essência estratégica, tática, logística e de pesquisa, prestando apoio e suporte ao planejamento das operações de guerra. Conforme explicitado na figura 2, as AGE são compostas pelo Reconhecimento Eletrônico (RETRON) e Aprestamento Eletrônico (APEL).

Figura 2: Estrutura das Atividades de Guerra Eletrônica.

Fonte: (MARINHA DO BRASIL, 2016a).

2.2.1.1 Reconhecimento Eletrônico (RETRON)

De acordo com Marinha do Brasil (2016a), o Reconhecimento Eletrônico é o conjunto de atividades de caráter estratégico, voltado ao planejamento de uma operação militar. O RETRON busca a obtenção, processamento contínuo e oportuno das informações provenientes dos sinais eletromagnéticos. Seus produtos são de caráter operacional/ tático ou estratégico: este está ligado às estimações da CGE do inimigo, viabilizando o preciso dimensionamento e proteção da nossa própria capacidade, provendo uma avaliação realista da sua adequabilidade e a aquisição de novos dados para a sua reformulação enquanto aquele, ao apoio ao planejamento de uma operação militar.

2.2.1.2 Aprestamento Eletrônico (APEL)

Segundo Marinha do Brasil (2016a), o Aprestamento Eletrônico é o conjunto de atividades que buscam fornecer os recursos de toda ordem necessários ao estabelecimento, verificação, manutenção ou reformulação da CGE, sendo pautada na Ciência, Tecnologia e Inovação (CT&I), Fomento Industrial, Formação de Pessoal, Manutenção e Reparo e Documentação. Tem na Formação de Pessoal sua principal base e fonte de recursos, envolvendo a qualificação e formação de pessoal para CT&I, indústrias de produção de sistemas de interesse da GE, mantenedores, pessoal operacional e analistas de RETRON.

2.2.2 Medidas de Guerra Eletrônica (MGE)

Conforme Marinha do Brasil (2016a) explica, as Medidas de Guerra Eletrônica, diferentemente das AGE, visam o efetivo emprego da CGE em uma opeação militar e são constituídas pelo somatório das Medidas de Apoio à Guerra Eletrônica (MAGE), Medidas de Ataque Eletrônico (MAE) e Medidas de Proteção Eletrônica (MPE), conforme apresentado na figura 3.

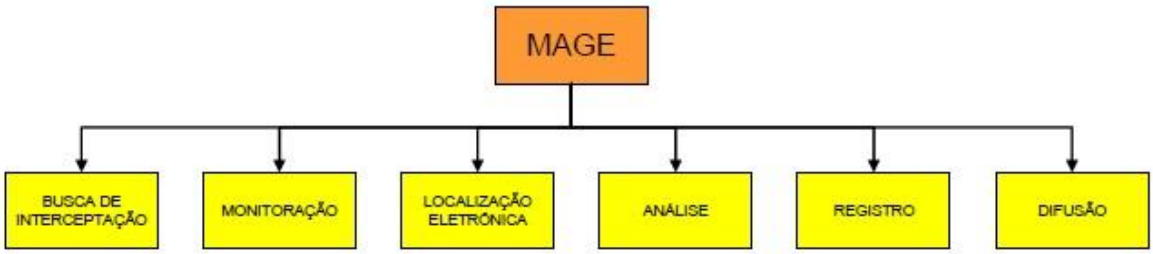
Figura 3: Subsivisões das Medidas de Guerra Eletrônica.

Fonte: (MARINHA DO BRASIL, 2016a).

2.2.2.1 MEDIDAS DE APOIO A GUERRA ELETRÔNICA (MAGE)

As MAGE, segundo Marinha do Brasil, (2016a) e Marinha do Brasil, (2016b), empreendem as ações visando à busca, interceptação, identificação e localização eletrônica das fontes de energia eletromagnética irradiada, de modo a permitir sua análise, o imediato reconhecimento de uma ameaça ou sua posterior exploração. Conforme ilustrado na figura 4, seu desenvolvimento ocorre de maneira sequencial, porém não exclusivamente nesta ordem, poden haver coincidencias de fases, especialmente nas fases de análise, registro e identificação, já que são funções de difícil separação em equipamentos automatizados, onde a interferência humana é reduzida.

Figura 4: Etapas das MAGE.



Fonte: (MARINHA DO BRASIL, 2016a).

Os resultados das ações de MAGE fornecem inúmeros dados e conhecimentos que contribuirão para a entrega de uma série de produtos tais como a identificação do nível de ameaça do contato, a determinação da posição, velocidade e o rumo de deslocamento da unidade que está realizando a emitição, as atividades e intenções do oponente e as características e qualidade do equipamento eletrônico empregado pelo oponente.

2.2.2.2 MEDIDAS DE ATAQUE ELETRÔNICO (MAE)

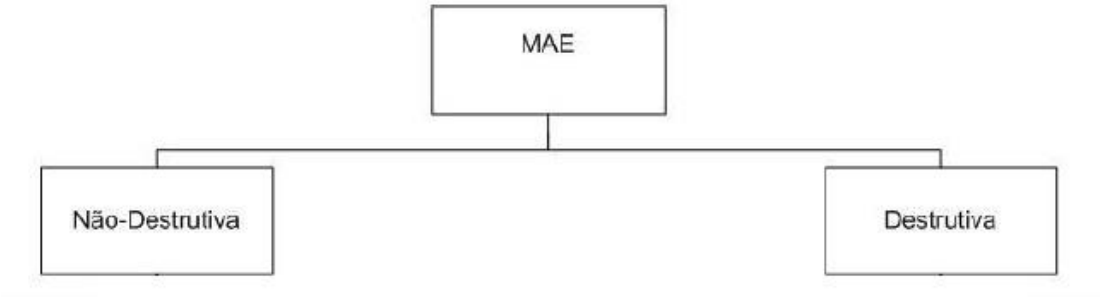
De acordo com Marinha do Brasil, (2016a) e Marinha do Brasil, (2016c), as Medidas de Ataque Eletrônico são o segmento da Guerra Eletrônica que compreende as ações cujas finalidades são reduzir ou evitar o uso efetivo do espectro eletromagnético pelo inimigo, além de destruir, neutralizar ou degradar a capacidade de combate do mesmo, usando energia eletromagnética ou armamento que empregue este espectro.

Ao pensar em fazer um bom planejamento do emprego das MAE, é de fundamental importância possuir o pleno conhecimento da capacidade de MAE da própria força. Possuem como objetivos principais impedir ou reduzir a capacidade de comunicações, identificação, detecção, navegação eletrônica do oponente e comando e

controle (C2), afetando também Sistemas de Aeronaves Remotamente Pilotados (SARP); neutralização ou diminuição da capacidade de sistemas de armas que empregam energia eletromagnética para a guiagem, comunicação, controle ou detonação, ampliando, assim, a proteção das nossas forças, o impedimento ou redução da capacidade do oponente de coleta e produção conhecimentos sobre nossas ações e a neutralização ou reduzução da velocidade do ciclo de decisão do oponente afetando o seu controle de ação planejada.

De acordo com a figura 5, as MAE estão divididas em dois grupos: MAE destrutivas (hard kill) e MAE não-destrutivas (soft kill).

Figura 5: Subdivisões das Medidas de Ataque Eletrônico.



Fonte: Adaptado de Marinha do Brasil (2016c).

A GE, considerada até pouco tempo atrás como um recurso voltado para defesa, vem perdendo essa característica. O motivo pelo qual isso vem ocorrendo está nas MAE destrutivas trazem consigo a capacidade de letalidade e destruição. Dentre as medidas destrutivas estão armas antirradiação e os dispositivos de energia direcionada.

Por outro lado, as MAE não-destrutivas utilizam o espectro eletromagnético, ativa ou passivamente, para lograr êxito em seu ataque eletrônico entretanto, sem causar nenhum tipo de dano ou destruição física ao oponente. Este tipo de MAE divididem-se em Supressão Eletromagnética, Despistamento Eletromagnético e Armas de Energia Direcionada.

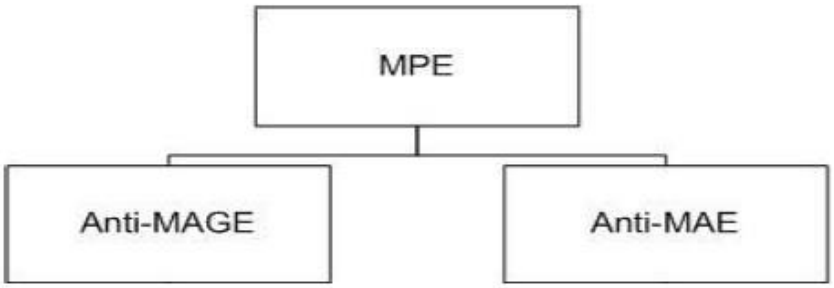
As MAE, quando bem sucedidas, resultam na redução da eficácia e eficiência das ações, tanto ofensivas quanto defensivas da força inimiga durante o tempo necessário. O desfecho de qualquer ataque terá maiores chances de sucesso caso o oponente seja bloqueado.

Ambas as formas de MAE podem afetar diversos sistemas de interesse militar, tais como de comunicações via dados, voz ou links, de acompanhamento e direção de tiro, navegação, vigilância, detecção, aquisição e identificação (radar, óptico) e detecção passiva (MAGE).

2.2.2.3 MEDIDAS DE PROTEÇÃO ELETRÔNICA (MPE)

Segundo Marinha do Brasil, (2016a) e Marinha do Brasil, (2016d), as Medidas De Proteção Eletrônica são o conjunto de ações tomadas com o intuito de proteger os equipamentos, sistemas, instalações, meios e pessoal, de modo a garantir o efetivo uso do espectro eletromagnético, visando à proteção frente à utilização das MAE de forças tanto amigas quanto inimigas. De acordo com a figura 6, as MPE se dividem em dois grupos: Anti-MAGE e as MPE Anti-MAE.

Figura 6: Estrutura das Medidas de Proteção Eletrônica.



Fonte: Adaptado de Marinha do Brasil (2016d).

Segundo Marinha do Brasil (2016d), as MPE têm como efeitos desejados a diminuição da capacidade de emprego, pelo inimigo ou por terceiros, de equipamentos os quais sejam capazes de interceptar as nossas emissões por meio do eficiente gerenciamento do espectro; a eliminação, redução e a otimização do emprego dos sistemas eletrônicos da Força, eliminando a interferência mútua; a negação da obtenção pelo inimigo ou por terceiros, de conhecimentos e localização de nossa força por meio do seu sistema de GE; e a redução do efeito das MAE dos oponentes.

As MPE anti-MAGE tem como objetivo principal negar, ao inimigo, a possibilidade de identificação, interceptação, a análise de nossas emissões e/ou localização através das MAGE, enquanto que as MPE anti-MAE tem por objetivo minimizar o efeito das MAE dos oponentes ou ainda os produtos da utilização das MAE por parte de Forças amigas, sobre nossos equipamentos.

Tanto quanto nas MAE e MAGE, um bom planejamento das MPE é um fator preponderante para o seu sucesso. E, para tal, conforme Marinha do Brasil (2016d) recomenda, devemos avaliar alguns pontos-chave tais como a distribuição das forças amigas no teatro de operações; meios amigos disponíveis; momento e forma de aplicação dos recursos amigos; os sistemas e equipamentos inimigos (MAGE e MAE) e os recursos e procedimentos alternativos.

3 METODOLOGIA

3.1 Classificação da Pesquisa

Este trabalho focou nos aspectos qualitativos do conteúdo a ser apresentado, enfatizando os conceitos fundamentais de cada tópico.

3.1.1 Quanto aos fins

Este trabalho, no que tange a natureza de sua metodologia, quanto aos fins, é exploratória, visto que busca proporcionar uma maior familiaridade com as técnicas e conceitos de GE, com maior foco nas MPE.

3.1.2 Quanto aos meios

Já quanto aos meios, esse trabalho deve ter sua pesquisa classificada como bibliográfica, tendo em vista que o desenvolvimento alcançado aqui foi consolidado pela busca em livros, artigos e monografias.

3.2 Limitações do Método

Devido ao caráter reservado deste trabalho e à elevada carga horária, não foi possível um maior aprofundamento no tema e na abrangência de técnicas.

3.3 Coleta e Tratamento de Dados

Para a realização deste trabalho, utilizou-se um arcabouço técnico composto por uma vasta pesquisa bibliográfica, utilizando-se de livros, artigos acadêmicos, monografias, dissertações e teses disponíveis em meio digital. O conhecimento obtido foi organizado de modo a estabelecer um raciocínio lógico e coerente, para apresentar e correlacionar os conceitos básicos do tema.

4 GUERRA ELETRÔNICA NAS COMUNICAÇÕES

4.1 Importância e Principais Medidas de Guerra Eletrônica

Segundo Spezio (2002), o domínio do EEM possui papel de extrema importância nos conflitos mundiais e o melhor uso da tecnologia que concede o controle deste espectro permite definir a vitória ou a derrota em um conflito militar. Tem como principal objetivo elevar o grau de confiabilidade e segurança das emissões, além de impedir ou dificultar o emprego das MAGE e MAE pelo oponente.

Os principais procedimentos que serão abordados por este trabalho são: Salto em Frequência, Bloqueio Eletrônico, Autenticação de Posto, Aproveitamento do Terreno, Antenas Direcionais e Padrão de Radiação, Mensagem Preestabelecida, Códigos de Nomes, Controle de Potência e Mudança de Polarização.

4.1.1 Bloqueio Eletrônico

De acordo com Marinha do Brasil (2016c), a técnica do pode ser definida como: “a deliberada irradiação, reirradiação ou reflexão de energia eletromagnética, com o propósito de restringir ou anular o desempenho de equipamentos ou sistemas eletrônicos em uso pelo oponente.” O objetivo de seu uso consiste em impedir, ou ao menos dificultar, a recepção dos sinais eletromagnéticos nos equipamentos de detecção oponentes, comunicações, navegação eletrônica, além dos sistemas de direção, controle de armas e sistema de armas e, ainda, de identificação eletrônica.

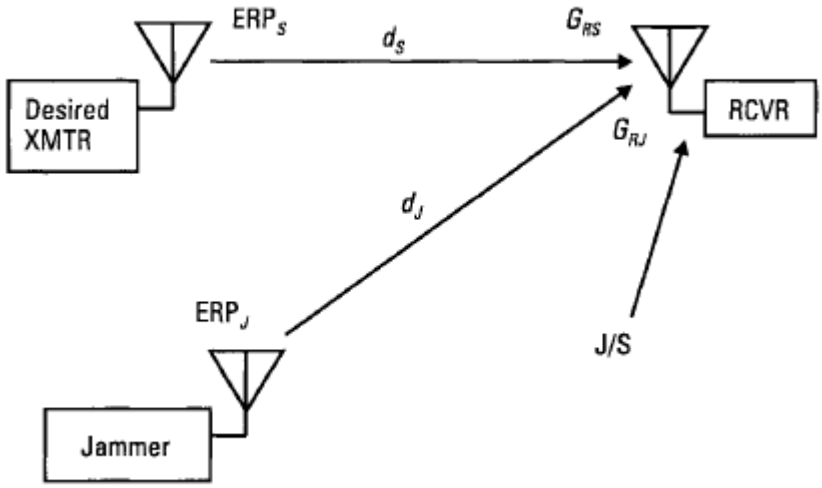
Os equipamentos os quais são usados na técnica de Bloqueio Eletrônico nada mais são que diversos tipos de transmissores, os quais foram projetados especialmente para realizar um bloqueio ou a introdução de sinais bloqueadores nos receptores do inimigo, podendo ser usados contra quaisquer tipos de equipamentos eletrônicos oponente, quer sejam de comunicações, sistemas de identificação, de radar, auxílio eletrônico à navegação ou de guiagem de mísseis.

Voltando para o âmbito das comunicações, segundo Da Silva (2009) e Soares (2018), o Bloqueio de Rádio Frequência (BRF) é uma maneira de inviabilizar um determinado tipo de comunicação com a emissão de outro sinal. Um dispositivo bloqueador insere no espectro eletromagnético, propositalmente, sinais interferentes nas frequências de

operação do sinal que se deseja bloquear, degradando a sua recepção. Sistemas como este são uma importante estratégia de defesa baseada na dissuasão.

Para obter uma eficiência máxima no BRF é importante obter informações sobre o teatro de ação, condições reinantes na atmosfera, em especial como será o comportamento da propagação de ondas eletromagnéticas, de modo a permitir a predição da área de cobertura esperada para o bloqueio, dependendo, diretamente, pela emissão do bloqueador e do sinal sinal a ser bloqueado. A Figura 7 demonstra ilustra tal fato.

Figura 7 - Representação da chegada do sinal do bloqueador.



Fonte: ADAMY (2006).

Ao analisar a Figura 7, constata-se que, no receptor, chegam sinais eletromagnéticos oriundos do bloqueador e do sistema de transmissão. O objetivo deste bloqueador é impedir o estabelecimento da comunicação por meio do seu sinal interferidor. Ressalta-se que o bloqueio é percebido somente pelo receptor e não em todo o sistema no qual ele está inserido, sendo, por esse motivo, difícil a comprovação de sua eficácia. De acordo com Marinha do Brasil (2016c), a ação de bloqueio, seja ela sofrida ou implementada, nunca deve ser mencionado quais foram seus resultados a outros países, quer seja em adestramentos ou em operações reais quando após atividades de provocação.

O bloqueio em comunicações, quanto ao método de execução, pode ser classificado em:

a) bloqueio de ponto;

b) bloqueio de barragem; e

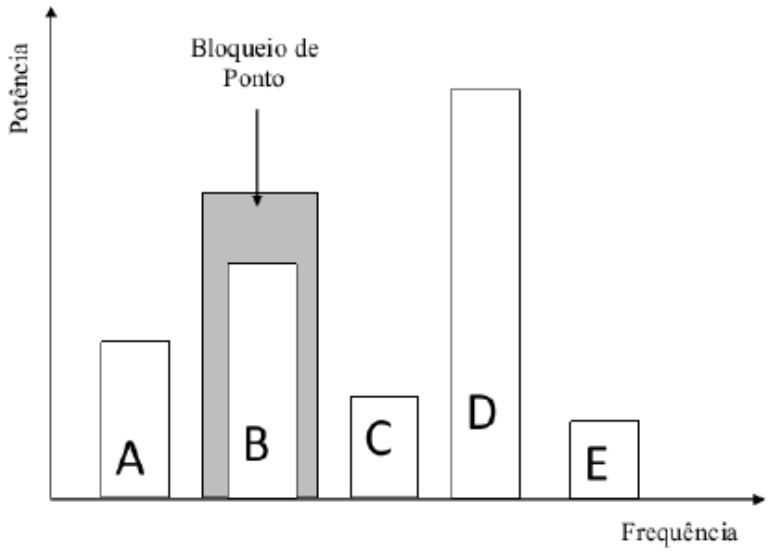
c) bloqueio de varredura.

4.1.1.1 Bloqueio de Ponto

De acordo com Marinha do Brasil (2016c), o bloqueio eletrônico de ponto utiliza transmissores os quais utilizam uma faixa estreita e sintonia precisa, podendo ser modulados em frequência ou amplitude e são empregados individualmente de acordo com cada equipamento do oponente que se deseja bloquear, atuando sobre a largura de banda ocupada pelo receptor do inimigo no espectro, e a eficiência desse bloqueio depende, diretamente, do conhecimento da frequência exata na qual o oponente está operando, o que pode ser obtido por ações de MAGE ou pelo RETRON.

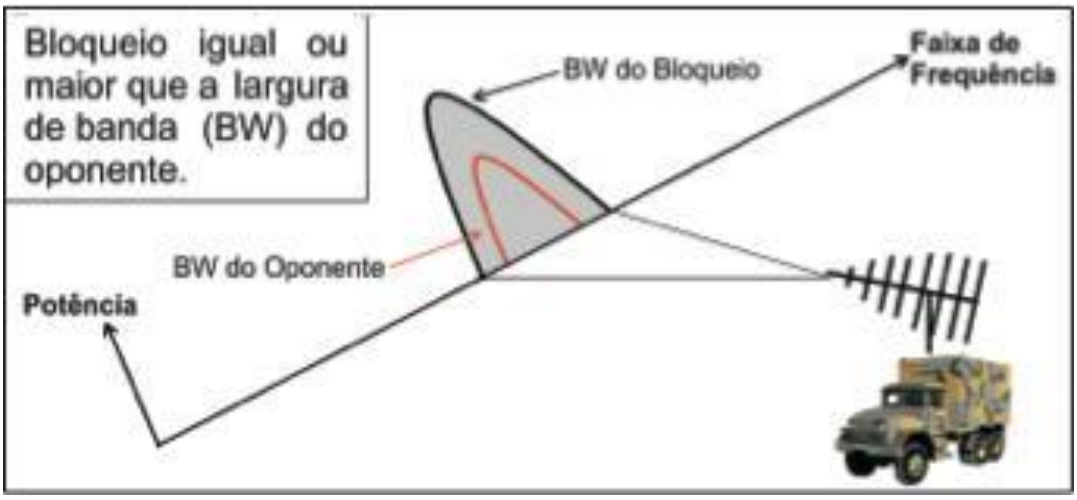
A principal vantagem deste tipo de bloqueio reside em concentrar uma grande energia numa faixa estreita de frequência, enquanto que sua maior limitação se dá na sua perda de eficiência no caso do inimigo mudar sua frequência de operação sendo necessárias novas ações de MAGE e RETRON para o descobrimento da nova frequência. A figura 8 exemplifica

Figura 8: Bloqueio de ponto



Fonte: (MARINHA DO BRASIL, 2016c).

Figura 9: Bloqueio de ponto



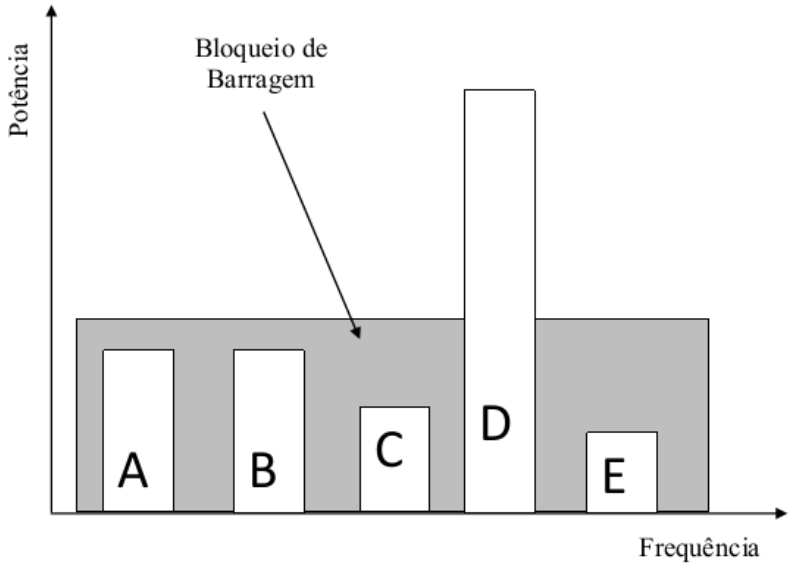
Fonte: (BRASIL, 2007).

4.1.1.2 Bloqueio de Barragem

De acordo com MARINHA DO BRASIL (2016c), o bloqueio de barragem realiza transmissão de energia eletromagnética em uma larga faixa de frequência, quando comparada com a largura de banda sintonizada pelo receptor inimigo, dificultando ou negando o seu emprego e a utilização de grande parte do espectro pelo oponente. Neste tipo de bloqueio, a largura de faixa é, normalmente, variável e, em alguns equipamentos, pode ser dividida em duas ou mais partes, dentro de sua faixa de bloqueio.

A principal vantagem deste tipo de bloqueio é a cobertura de uma larga faixa de frequência, ou seja, bloqueia várias frequências e equipamentos simultaneamente e a capacidade de cobrir toda a gama de radares que podem aplicar a técnica de agilidade em frequência. Dentre as desvantagens desse método, ressaltam-se a perda de densidade (baixa concentração) de potência no bloqueio, uma vez que estará distribuída sobre uma grande faixa de frequência, possibilidade de apresentar pontos de bloqueio com intensidade baixa ou nula. Outro ponto negativo deste tipo de MAE é a impossibilidade de realizar um bloqueio em um equipamento oponente quando este estiver operando em frequência próxima à de um equipamento da força amiga, sem ocorrer o bloqueio deste também, tornando-o, muitas vezes, inadequado dependendo da situação.

Figura 10: Bloqueio de barragem



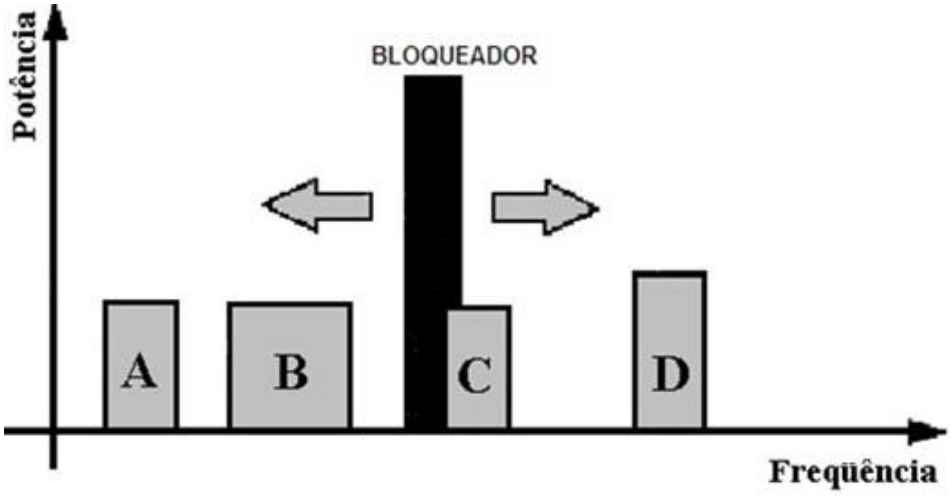
Fonte: (MARINHA DO BRASIL, 2016c).

4.1.1.3 – Bloqueio de Varredura

Este tipo de bloqueio utiliza transmissores de faixa estreita com grande concentração de potência, com sintonia variável, o sinal bloqueador executa uma varredura em frequências selecionadas. A vantagem deste tipo de bloqueio é a cobertura de um grande número de frequências pré-selecionadas, sem a perda de densidade de potência.

Trata-se, basicamente, de um bloqueio multifunção, o qual é produzido por um equipamento capaz de realizar dois ou mais tipos de bloqueio simultaneamente. Pode, ainda, impor uma descontinuidade no bloqueio ou inserir uma informação falsa (dissimulação).

Figura 11: Bloqueio de varredura



Fonte: Disponível em https://slideplayer.com.br/slide/1625694/. Acesso em: 17/04/2021.

4.1.2 Autenticação de Posto

Segundo Aguiar (2018), a autenticação de posto tem o intuito de verificar se o posto transmissor ou receptor pertence à força amiga ou inimiga. Consiste numa medida de segurança que busca proteção contra transmissão ou mensagens falsas introduzidas pelo inimigo com o propósito de induzir ações erradas, confundir ou descobrir conteúdo de mensagens importantes.

Sendo assim, será solicitada a autenticação do posto quando houver desconfiança de uma ação de Despistamento Imitativo, MAE que consiste em, se passando por força amiga, o inimigo dissemina uma mensagem falsa na rede..

Na prática, esse tipo de medida de segurança ocorre comumente na Marinha do Brasil, tanto quanto uma força se faz ao mar através de tabelas de autenticação constantes nos documentos da missão quanto em Organizações Militares em apoio ou de Fuzileiros Navais por meio de senha e contra-senha.

Diversos fatores podem levar a um pedido de Autenticação do Posto tais como uma ordem na rede que fuja dos padrões anteriores, ordens de deslocamento fora do contexto previsto da missão ou que solicitem informações sobre a operação, a desconfiar da voz do seu interlocutor, mensagens sendo transmitidas em claro, a realização de uma transmissão direcionada a uma estação a qual esteja em condição de silêncio eletrônico, o estabelecimento ou o encerramento dessa condição de silêncio ou sempre que houver alguma suspeita sobre a autenticidade de uma transmissão.

4.1.3 Aproveitamento do Terreno

Esta técnica se baseia em considerar, ao se alterar o posicionamento de uma estação ou antena, a existência de obstáculos no terreno os quais possam vir a dificultar as AGE inimigas, tais como prédios, rede elétrica de alta tensão, montanhas, florestas e matas densas.

Segundo Aguiar (2018), recomenda-se que a escolha das posições adotadas seja, se possível, de forma que o obstáculo esteja entre a estação e a emissão do inimigo, de modo a prservar a onda eletromagnética dos fenômenos de reflexão, absorção e refração, aproveittando, em partes, o bloqueio mecânico (bloqueio por meio de algum material com a intenção de prejudicar ou interromper a propagação das ondas eletromagnéticas) como uma medida de proteção.

Figura 12: Aproveitamento do Terreno

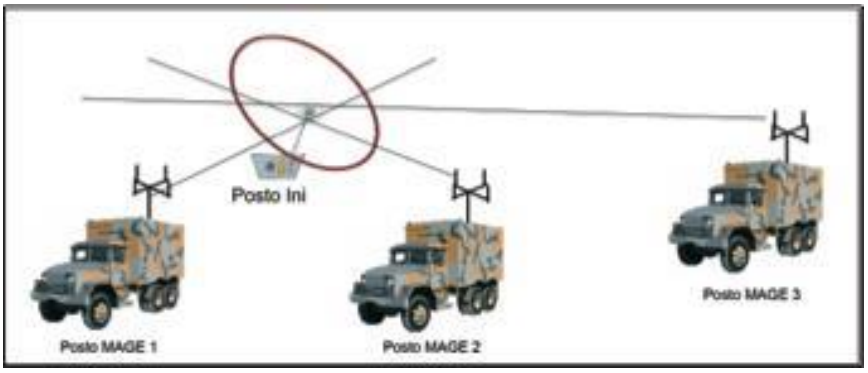
Fonte: Disponível em https://www.army.mil/article/226082/army_showcases_new_electronic_warfare_tech. Acesso em: 17/04/2021.

4.1.4 Antenas Direcionais e Padrão de Radiação

Segundo Aguiar (2018) Antenas direcionais que emitam paralelamente em relação ao inimigo evitam a recepção MAGE pela força oponente, logo evita a determinação da posição (conhecido como Localização Eletrônica) de quem estiver emitindo, e amenizam ações MAE sobre os equipamentos que se desejam proteger.

A localização eletrônica pode ser dificultada pelo uso de antenas direcionais, pois aquela utiliza como informação básica a direção de chegada. Então, receptores obtém direção e sentido das emissões, localização horizontal, ou direção e altura da ionosfera, localização vertical, para indicar localização provável do emissor.

Figura 13: Localização horizontal



Fonte: BRASIL(2007)

Recomenda-se o paralelismo de emissão quando à frente do inimigo, entretanto, evitar seu uso na direção perpendicular, e, se possível, emitir apenas na direção da estação de interesse.

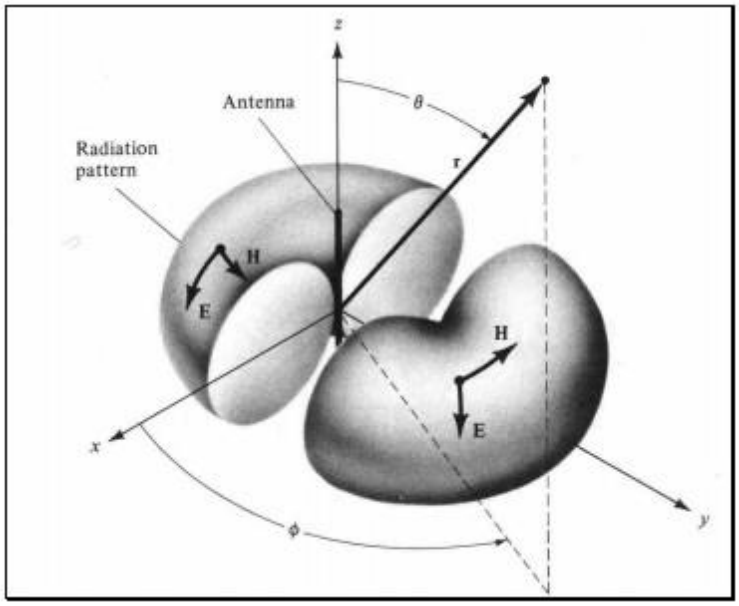
É de grande importante ressaltar que o direcionamento incorreto das antenas pode acarretar em falha nas comunicações além da impossibilidade de criar além de um enlace entre estações com marcações diferentes por causa da direcionalidade das antenas.

Segundo a definição utilizada pelo Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE) o padrão de radiação é a distribuição espacial de uma quantidade que caracteriza o EEM gerado por uma antena. Essa distribuição espacial pode ser expressa por meio de uma função matemática ou de uma representação gráfica.

Segundo Soares (2018), o padrão de radiação é dividido duas classes: omnidirecional e direcional. As antenas omnidirecionais são aquelas usadas quando se pretende fazer uma cobertura em todas as direções horizontais e possuem uma cobertura vertical variável. A Figura 14 apresenta o padrão de distribuição espacial da radiação de uma antena omnidirecional

As antenas omnidirecionais possuem, como principal vantagem, a característica de o sinal transmitido cobrir toda região em torno do transmissor, favorecendo, sobremaneira, a sua chegada no receptor. Entretanto, no que tange sua aplicação no meio militar, essa característica torna-se um risco, pois facilita que o inimigo detecte o sinal transmitido.

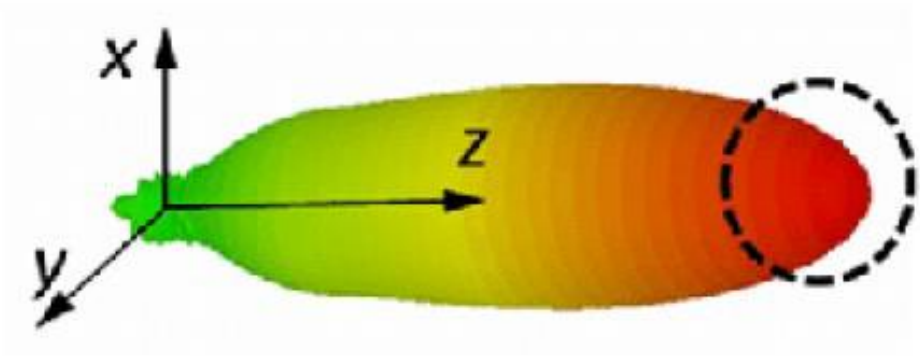
.Figura 14 – Padrão de distribuição espacial de radiação de uma antena omnidirecional.



Fonte: Fernandes (2002).

Antenas direcionais, por sua vez, possibilitam a escolha do azimute de posicionamento e após esta seleção, este tipo de antena mantém uma direção fixa para transmissão e recepção de sinal conforme representado na figura 15. Pode-se notar que a sua transmição possui uma direção totalmente definida, não estando disponível horizontalmente nos 360°, dificultando, assim, que o sinal seja interceptado pelo oponente. Entretanto, para se estabelecer a comunicaçãoatravés de antenas com o padrão de radiação direcional é preciso conhecer uma informação nem sempre disponível: a localização do receptor.

Figura 15 - Padrão de Radiação Direcional.



Fonte: Huang (2015).

4.1.5 Mudança de Polarização

Segundo Electronic Warfare Fundamentals (2000) e Aguiar (2018), é extremamente relevante queas antenas de transmissão entre duas estações as quais desejam se comunicar estejam com a mesma polarização a fim de minimizar as perdas. Este fundamento também é utilizado pela antena MAGE em relação ao emissor de interesse.

Ao analisar a tabela 1, notamos o impacto da polarização conforme algumas combinações de antenas de transmissão e de recepção selecionadas. Observa-se que, polarizações defasadas de 90^{o} acarretam enormes perdas de sinais. Como medida corretiva, pode-se alterar a polarização da antena, ou sua inclinação e, desta forma, reduzir-se-ia as perdas de propagação devido à polarização das antenas.

Dessa forma, a polarização das antenas pode funcionar como uma contra medida para evitar interceptação por MAGE, ou quando se estiver em passivo por MAE, por exemplo.

Tabela 1 – Perda por polarização da antena

Transmissor Polarização da Antena	**Receptor** Polarização da Antena	Percentual de perda
Vertical	Vertical	0
Vertical	Inclinação (45^o ou 135^o)	50
Vertical ou Horizontal	Horizontal ou Vertical	75
Horizontal	Horizontal	0
Horizontal	Inclinação (45^o ou 135^o)	50

Fonte: Adaptado de Electronic Warfare Fundamentals (2000)

4.2 Tecnologias de Medidas de Proteção Eletrônica

Neste tópico, serão apresentadas tecnologias utilizadas nos sistemas eletrônicos como MPE as Comunicações contra MAGE ou MAE oponentes.

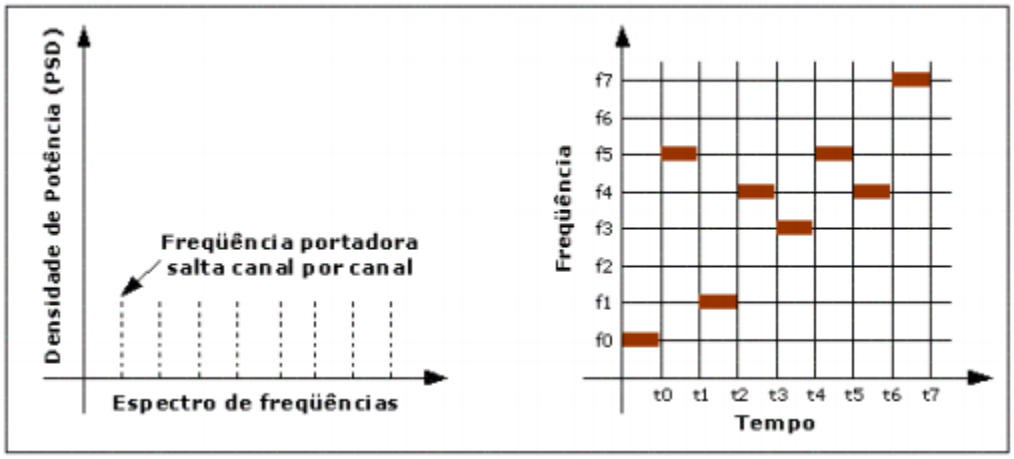
4.2.1 Salto em Frequência

Segundo o livro Electronic Warfare Fundamentals (2000), o salto em frequência é uma técnica onde o valor da "frequência da portadora das transmissões pulsadas é periodicamente ou continuamente deslocada dentro dos limites de cada pulso" (ELECTRONIC, 2000).

Em consonância com (FERNANDES, 2002) (SOARES, 2018), essa técnica realiza a mudança sistêmica da portadora, utilizando-se de diferentes canais de frequência, essa troca é realizada por meio de um gerador de códigos "pseudo-randômico", o qual gera códigos que parecem aleatórios mas que, na verdade, não o são, pois estão sendo gerados a partir de um processo determinístico.

Para que o receptor consiga receber a informação transmitida é preciso que o mesmo monitore os canais de frequência definidos pela sequência "pseudo-aleatória" (FERNANDES, 2002). Como é ilustrado pela Figura 16.

Figura 16 - Técnica empregada na tecnologia de saltos em frequência.



Fonte: (SOARES, 2018).

Presente em equipamentos mais modernos, é necessário que, durante a execução desta técnica, todas as estações estejam sincronizadas quanto as mudanças de frequência de modo a manter a continuidade no tráfego de mensagens.

O salto em frequência pode ser classificado como uma MPE, pois é uma medida adotada para garantir o uso do EEM pela própria força.

4.2.2 Controle de Potência

De acordo com SOARES (2018) ponto chave para o controle de potência de transmissão é saber a localização dos Rádios Receptores de Interesse (RRI), quando essa informação é conhecida é fundamental utilizar somente a potência necessária, caso contrário é desejável não utilizar potências muito elevadas quando o equipamento permite realizar tal controle.

Segundo (TEIXEIRA, 2009) e (SOARES, 2018), para saber o valor da potência que o equipamento rádio receptor irá receber o sinal transmitido, o modelo de propagação no espaço livre é utilizado, ele permite calcular qual potência a empregar dependendo da posição do RRI. Considerando que entre transmissor e receptor existe um meio onde não há obstrução da linha de visada direta entre as duas antenas. Assim, temos que:

$$P_R(d) = \frac{PtGtGr\lambda^2}{(4\pi)^2 d^2} \qquad (1)$$

Onde:

Pr – potência recebida;

Pt – potência transmitida;

Gt – ganho da antena transmissora;

Gr – ganho da antena receptora;

λ – comprimento de onda; e

d – distância entre o transmissor e o receptor (em metros).

Com uma análise da Equação (1) é possível tirar como conclusão que a potência recebida Pr é diretamente proporcional à potência de transmissão, aos ganhos da antena transmissora e da antena receptora, ao quadrado do comprimento de onda e inversamente proporcional ao quadrado da distância.

De acordo com (TEIXEIRA, 2009), as perdas de propagação sofridas pelo sinal, medida em dB, é expressa por:

$$L_{TOTAL}(dB) = 10\log\left(\frac{Pt}{Pr}\right) = -10\log\left(\frac{GtGr\lambda^2}{(4\pi d)^2}\right) \quad (2)$$

Se a antena em estudo for omnidirecional, tanto na transmissão quanto na recepção (GT = GR = 0, em dB), teremos:

$$L_{TOTAL}(dB) = 10\log\left(\frac{Pt}{Pr}\right) = -20\log\left(\frac{\lambda}{4\pi d}\right) \quad (3)$$

É possível notar que, a partir da equação 1, a atenuação para uma antena que possua um padrão de irradiação omnidirecional é diretamente proporcional ao quadrado do seu comprimento de onda e inversamente proporcional ao quadrado da distância entre o transmissor e receptor. Assim quanto mais distante se estiver, mais potência deve ser utilizada.

De acordo com (SAARNISAARI, 2017) e (SOARES, 2018), é importante que o sinal recebido possua relação sinal ruído (SNR) que permita identificar de maneira adequada a informação recebida, a SNR é dada por:

SNR = (Potência do Sinal)/(Potência do Ruído) (4)

Comparando as equações (1), (2), (3) e (4), em consonância com (SOARES, 2018), é possível notar que aumentando a distância, a potência recebida do sinal diminui e a relação sinal ruído diminui, considerando o ruído aproximadamente constante. Logo, pode-se concluir que caso se tenha a localização dos RRI é importante controlar a potência de transmissão para que o sinal possua uma relação sinal ruído baixa, dificultando a interceptação do sinal por forças inimigas. Porém, caso não se tenha essa localização o controle da potência de transmissão irá depender da necessidade, sendo recomendado não transmitir com potências muito elevadas. Esse controle da potência de transmissão é uma MGE, que se enquadra como MPE, pois é uma ação para a proteção.

Essa técnica de controle de potência pode ser feita manualmente pelo operador, assim, sendo caracterizado como procedimento de MPE; ou automaticamente, caso o equipamento possua essa tecnologia.

O emprego de baixa potência para transmissão em comunicações pode ser considerado uma medida Anti-MAGE, porque, possuindo um sinal baixo, dificulta a recepção.

4.2.3 Criptografia

Segundo (ARAÚJO, 2013) criptografia é o nome que se dá a técnicas que transformam uma informação inteligível em algo que um agente externo seja incapaz de compreender. Para que se possa estabelecer uma comunicação de forma segura em um contexto civil ou militar é preciso garantir que algumas propriedades sejam estabelecidas pelo sistema criptográfico utilizado.

1. Autenticidade: Garantir a identidade de cada um dos participantes de uma comunicação, de modo que não haja nenhum intruso tentando se passar por outro usuário;
2. Confidencialidade: Garantia de que só usuários autorizados tenham acesso a todas as informações trafegadas ou armazenadas em um sistema computacional ouu um arquivo;
3. Integridade: Garantia de que a informação que for trafegada em um determinado canal, durante a comunicação, chegará ao seu destino sem nenhum dado adulterado, ou seja, exatamente da mesma forma que partiu da origem; e

4. Irretratabilidade (ou não repúdio): Garantia de que tanto o remetente quanto o receptor das informações possam negar, posteriormente, a transmissão, recepção ou posse.

Usualmente, para se realizar a criptografia, são utilizadas chaves criptograficas e, estas, estão divididas em simétricas e assimétricas.

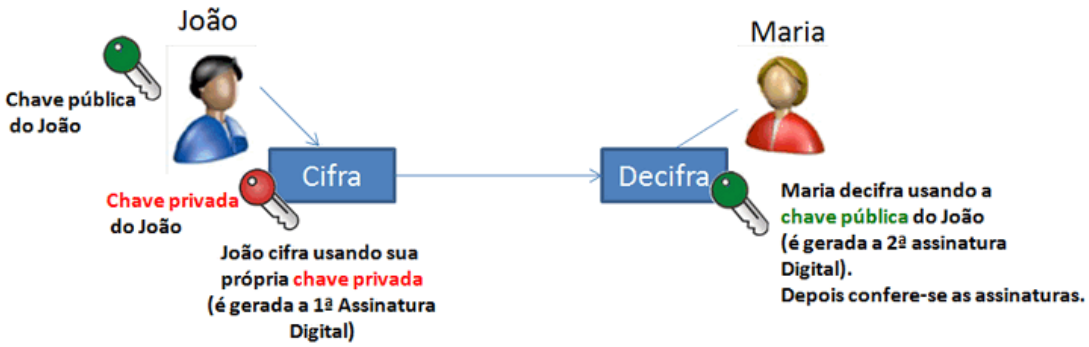
- Criptografia com chave simétrica: é utilizada uma única chave tanto para criptografar como para descriptografar. Porém, a principal vulnerabilidade dessa técnica reside no caso de descoberta da chave por terceiros, pois permitirá o acesso a informação conforme exemplificado na figura 17.

Figura 17 – Criptografia simétrica.

Fonte: Disponível em https://jkolb.com.br/criptografia-simetrica/. Acesso em: 17/04/2021.

- Criptografia com chave assimétrica: são utilizadas chaves diferentes para criptografar e descriptografar, garantindo, assim, com maior confiança a autenticidade e não-repúdio à mensagem como exemplifica a figura 18.

Figura 18 – Criptografia assimétrica.



Fonte: Disponível em https://www.rtell.com.br . Acesso em: 17/04/2021

4.2.4 Criptofonia

A utilização de sistemas de criptofonia tem como marco inicial a Primeira Guerra Mundial. Em decorrência dos conflitos posteriores, estes sistemas começaram a ser utilizados por Governos, Forças Armadas, companhias telefônicas e Missões Diplomáticas.

Com o advento dos semicondutores, foi possível construir sistemas de criptofonia mais seguros e que podiam operar de maneira mais amigável e, estes sistemas, de uma maneira geral, podem ser divididos em duas grandes classes: Cifradores Analógicos ou Misturadores e Cifradores Digitais.

Os cifradores analógicos apresentam níveis de segurança que variam de casual a táctico e devem ser empregados somente em situações que não exijam níveis de segurança estratégicos. Já os cifradores digitais são conhecidos como sistemas de criptofonia digital ou sistemas COMSEC e apresentam níveis de segurança mais elevado e qualificado.

Estes sistemas, ao invés de transmitirem partes do sinal de voz, enviam apenas os parâmetros produzidos na fase de análise do processo de codificação, o que permite a aplicação direta de técnicas de criptografia ao conjunto de parâmetros citado. Os cifradores digitais podem ser classificados em duas modalidades:

- Categoria I - Informação codificada na forma digital e transmissão não-codificada na forma analógica; e
- Categoria II – Informação e transmissão codificada (digital).

Este tipo de cifrador se beneficia da capacidade do transmissor de receber dados no formato digital e, desta forma, fornece o sinal encriptado diretamente ao modulador. Independentemente da classe do sistema de criptofonia utilizado, alguns requisitos importantes devem ser atendidos: Largura de banda do sinal crifrado compatível com o canal de transmissão utilizado; O sinal cifrado (voz) deve ser ininteligível ao ouvido humano, o que é equivalente a uma baixa inteligibilidade residual.

Para interpretar a mensagem transmitida, é fundamental que o receptor tenha a chave criptográfica. Devido a isso, pode ser considerado um recurso anti-MAGE uma vez que dificulta o acesso ao conteúdo da mensagem pelo inimigo. Embora não furte uma ação de localização ou bloqueio eletrônico.

4.2.5 Esteganografia

Como apresenta AGUIAR (2018), ao se considerar uma mensagem a ser transmitida por meio computacional, um arquivo comum, a técnica de Esteganografia consiste em esconder, mascarar ou ocultar a existência de uma mensagem (áudio, texto, imagem ou vídeo) dentro de outra mensagem, esta, porém, com conteúdo explícito que despiste o cenário, situação real da mensagem oculta, podendo ser empregada em impressoras modernas através da inserção de pequenos pontos amarelos adicionados a cada página contendo codificado o número de fabricação da impressora e a data da impressão; técnicas de filtragem; mascaramento de informações serviços de inteligência e marcas d'água conforme exemplificado nas figuras 19 e 20.

Figura 19 - Técnica de esteganografia codificando uma impressão.

Fonte: Disponivel em: https://www.gta.ufrj.br/ensino/eel878/redes1-2016-1/16_1/esteganografia/#aplicacoes

Figura 20 - Técnica de esteganografia com diversas codificações.

Fonte: Disponivel em: https://www.gta.ufrj.br/ensino/eel878/redes1-2016-1/16_1/esteganografia/#aplicacoes. Acesso em: 17/04/2021

Para que o destinatário possa ter acesso a essa mensagem implícita, é necessário que se tenha o programa ou a chave criptográfica correspondente. Isto dificulta a análise MAGE pelo oponente que a intercepte caso este não tenha as ferramentas corretas para descobrir a mensagem.

5 CONCLUSÃO

Neste trabalho foram abordados as teorias de GE com exemplos e teorias, métodos que aumentam a segurança na utilização de MPE nas comunicações, tanto contra Medidas de Ataque Eletrônico quanto contra Medidas de Apoio à Guerra Eletrônica.

Após aprofundar os estudos, é de fundamental importância que, o papel dos militares envolvidos na comunicação militar seja constante e intensamente treinados para que estejam aptos a utilizarem as tecnologias em constante evolução nos equipamentos, de modo que sejam capazes de colocar em prática os procedimentos de forma acertiva.

Conclui-se que, mantendo o nível de adestramento elevado, estando atentos às constantes evoluções das técnicas de GE, as melhores formas de se contrapor a uma ameaça é a eficente utilização das técnicas Anti-MAGE e Anti-MAE aliados ao emprego das MPE.

5.1 Sugestões para Futuros Trabalhos

Por se tratar de uma área em constante evolução e desenvolvimento, todo estudo ainda terá desdobramentos, sendo uma fonte inesgotável de lições. Como sugestão, fica o constante aprofundamento do tema proposto e em todas as áreas da Guerra Eletrônica.

REFERÊNCIAS

ANDRADE JR, José Francisco de. Speech Privecy for Modern Mobile Communication Systems. **Programa de Engenharia Elétrica – UFRJ**, 2008. Disponível em: <http://pee.ufrj.br/teses/index.php?Abstract=2008102201> Acesso em: 16 de abr. de 2021.

ADAMY, David L. **Introduction to communication electronic warfare systems**. Norwood: Artech House, 2002.

ADAMY, David L. **EW 102: A second course in electronic warfare**. Norwood: Artech House, 2004.

ADAMY, David L. **Introduction to Electronic Warfare Modeling and Simulation**. Norwood: Artech House, 2006.

ADAMY, David L. **EW 103: Tactical battlefield communications electronic warfare.** Norwood: Artech House, 2009.

ADAMY, David L. **EW 104: electronic warfare against a new generation of threats.** Norwood: Artech House, 2015.

AGUIAR Luiz Paulo Dos Santos de. **Guerra Eletrônica Nas Comunicações**: Suas Possibilidades Aplicadas À Defesa. Monografia (Curso de Aperfeiçoamento Avançado em Guerra Eletrônica), CIAW, Rio de Janeiro, 2018.

BRASIL. Ministério da Defesa. **Manual de Guerra Eletrônica para Emprego em Operações Combinadas**. MD32-M-02, 2007.

BRASIL. Diretoria-Geral do Material da Marinha. **DGMM-540: Normas de Tecnologia da Informação da Marinha.** 2 rev. Rio de Janeiro, 2017.

BRASIL. Ministério da Defesa. **Manual de Guerra Eletrônica para Emprego em Operações Combinadas.** MD32-M-02, 2007.

Comando de Operações Navais. **ComOpNav-521 – Manual de Guerra Eletrônica.** Rio de Janeiro, 2003.

Electronic Warfare Fundamentals, November 2000. Disponível em: <http://ebookbrowse.com/electronic-warfare-fundamentals-pdf-d1492716> Acesso em: 12 de abr. de 2021.

ESTADO MAIOR DA ARMADA (EMA). **EMA-305 Doutrina Básica da Marinha**. Brasília, DF, 2014.

EXÉRCITO BRASILEIRO. **Biblioteca Digital do Exército**, 2021. Disponível em: <https://bdex.eb.mil.br/jspui/handle/1/890> Acesso em: 15 de abr. de 2021.

FERNANDES, J. J. G. **Implementação de Espalhamento Espectral por Sequência Direta.** 2002. f. 141. Dissertação (Mestrado em Engenharia Elétrica) - Universidade Federal do Rio Grande do Sul, Porto Alegre, 2002. Disponível em: http://www.lume.ufrgs.br/handle/10183/3582. Acesso em 20mar. 2021.

HARGER, Campestrini Lucas. **Medidas de Ataque e Proteção Eletrônica para Receptores Navstar-Gps**. Monografia (Curso de Aperfeiçoamento Avançado em Guerra Eletrônica),

CIAW, Rio de Janeiro, 2018.

ITO, Christian Toshio. **O Futuro dos Navios-Escolta**. Revista Passadiço. Rio de Janeiro, ano 32, ed.39, p. 20 – 24, 2019.

MARINHA DO BRASIL. **GE 101 Conceitos Básicos de Guerra Eletrônica**. Centro de Guerra Eletrônica da Marinha. Rio de Janeiro, RJ, 2016a.

MARINHA DO BRASIL. **GE 102 Introdução às Medidas de Apoio à Guerra Eletrônica**. Centro de Guerra Eletrônica da Marinha. Rio de Janeiro, RJ, 2016b.

MARINHA DO BRASIL. **GE 103 Introdução às MAE**. Centro de Guerra Eletrônica da Marinha. Rio de Janeiro, RJ, 2016c.

MARINHA DO BRASIL. **GE 104 Medidas de Proteção Eletrônica**. Centro de Guerra Eletrônica da Marinha. Rio de Janeiro, RJ, 2016d.

PASSOS, Ana Paula Rocha Soares; BARBOSA, Anderson de Souza; CABRAL, Lucas Ferreira. **Esteganografia e Ofuscação**. Grupo de Teleinformática e Automação – UFRJ, 2016. Disponível em: <https://www.gta.ufrj.br/ensino/eel878/redes1-2016-1/16_1/esteganografia/#aplicacoes> Acesso em: 16 de abr. de 2021.

SAARNISAARI, H. **Future Military Mobile Radio Communication Systems from Electronic Warfare Perspective.** IEEE Xplore, Oulu, 2017. Disponível em: http://ieeexplore.ieee.org/document/7956494/. Acesso em 15 Abr. 2021.

SILVA, Alex Alvarez da. **Simulação e análise da eficácia das técnicas de bloqueio em sistemas de comunicações**: ênfase no sistema GSM. 2009. Dissertação (Mestrado em Engenharia Elétrica) - Instituto Militar de Engenharia, Rio de Janeiro, 2009.

SPEZIO, E. A. **Electronic Warfare Systems**. IEEE Xplore, Nova York, V. 50, n. 3, p. 633-643.

MINISTÉRIO DA DEFESA. Portaria Normativa no 333/MD, de 24 de março de 2004. **Dispõe sobre Política de Guerra Eletrônica de Defesa**. Diário Oficial da União no 59, Brasília, DF, 26 de março de 2004.

Oliveira, Humberto José Corrêa de. **Coletânea Histórica da Guerra Eletrônica.** Brasília: Centro Integrado de Guerra Eletrônica, Vol.3, 1ª Edição, 2006.

SOARES, Willian Sathler Lino. **Análise de Rádios Móveis de Comunicação com Enfoque em Guerra Eletrônica e Aplicação de Software para a Predição de Área de Cobertura de Sinais de Radiofrequência em VHF no Apoio ao Planejamento da Guerra Eltrônica**. Monografia (Curso de Aperfeiçoamento Avançado em Guerra Eletrônica), CIAW, Rio de Janeiro, 2018.

TEIXEIRA, R. B. M. **Predição do Sinal em uma Rede Local sem Fio através de Redes Neurais Artificiais**, 2009. Monografia (Graduação em Engenharia de Teleinformática) – Universidade Federal do Ceará, Fortaleza, 2009. Disponível em: http://www.cgeti.ufc.br/monografias/RICARDO_BRUNO_MARTINS_TEIXEIRA.pdf. Acesso em 11 Abr. 2021.