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 NAS COMUNICAÇÕES: suas possibilidades aplicadas à defesa

1TEN LUIZ PAULO DOS SANTOS DE AGUIAR

Rio de Janeiro
2018

1TEN LUIZ PAULO DOS SANTOS DE AGUIAR

GUERRA ELETRÔNICA NAS COMUNICAÇÕES: suas possibilidades aplicadas à defesa

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

Orientadores:
CC Robson Ribeiro Carreira
Erasmus Miranda, Ph.D.

CIAW
Rio de Janeiro
2018

FOLHA DE APROVAÇÃO

1TEN LUIZ PAULO DOS SANTOS DE AGUIAR

GUERRA ELETRÔNICA NAS COMUNICAÇÕES: suas possibilidades aplicadas à defesa

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

Aprovada em __ de junho de 2018.

Banca Examinadora:

Erasmus Miranda, P.h.D – PUC-Rio _____

CC Robson Ribeiro Carreira, MSc – CIAW _____

CMG (RM1-EN) Gian Karlo Huback Macedo de Almeida, MSc – CIAW _____

CIAW
Rio de Janeiro
2018

Dedico este trabalho a minha amada esposa Nathali, pela motivação, carinho e orações. Deus está conosco.

AGRADECIMENTOS

Primeiramente, toda glória seja dada a Jesus, meu Mestre, meu cabeça durante todo o curso, conforme está escrito: o temor do SENHOR é o princípio da sabedoria.

Agradecer aos meus pais, Luiz Carlos e Angela Maria, e à esposa, Nathali Brandão, que souberam compreender a minha ausência nas horas dedicadas ao curso.

Ao Capitão de Corveta Robson Ribeiro Carreira, pela atenção dispensada, paciência e excelente atuação como orientador técnico.

Ao professor Erasmus Miranda, meu orientador acadêmico, pelo incentivo constante, objetividade e assistência.

Ao professor Fernando da Rocha Pantoja, que transmitiu os conhecimentos necessários para a conclusão do curso e deste trabalho com muita competência e dedicação.

Ao CIAW, pelo conhecimento científico adquirido.

A todos os meus camaradas e amigos do curso de Guerra Eletrônica pelos bons momentos partilhados, pela ajuda e pela amizade.

A todas as pessoas que, direta ou indiretamente, contribuíram para a execução desta Monografia.

"O céu e a terra passarão, mas as minhas palavras não hão de passar."
Mateus 24:35

GUERRA ELETRÔNICA NAS COMUNICAÇÕES: suas possibilidades aplicadas à defesa

Resumo

Meios eletrônicos são extremamente relevantes na propagação de informações, tanto para transmissão de ordens à tropa ou aos meios navais quanto para controle do sistema de armas. O presente trabalho apresenta métodos para emprego de meios eletrônicos de forma mais eficaz em um teatro de operações que se pode considerar hostil quanto ao uso do espectro eletromagnético (EEM).

Palavras- chave: segurança; proteção; ataque.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTAS DE SIGLAS E ABREVIATURAS

DBM	Doutrina Básica da Marinha
CGE	Capacidade de Guerra Eletrônica
Com	Comunicação
EB	Exército Brasileiro
EEM	Espectro Eletromagnético
END	Estratégia Nacional de Defesa
FFAA	Forças Armadas
GE	Guerra Eletrônica
MAE	Medidas de Ataque Eletrônico
MB	Marinha do Brasil
MAGE	Medidas de Apoio a Guerra Eletrônica
MPE	Medidas de Proteção Eletrônica
NCom	Não-Comunicação
OM	Organização Militar
PTT	Push to talk

SUMÁRIO

1. INTRODUÇÃO

1.1 Aspectos da Evolução Tecnológica

O avanço da tecnologia alcançou os equipamentos utilizados na Guerra Eletrônica (GE). Podemos encontrar equipamentos que trabalham ininterruptamente, multiplexação de tarefas, maior eficácia na identificação de emissões , tempo de realização de atividades foram reduzidos a segundos são alguns exemplos dos reflexos desse avanço tecnológico.

Isso nos faz rever Medidas de Proteção Eletrônica (MPE) que não estejam defasadas a essas mudanças tecnológicas uma vez que o aumento do processamento de dados e automação de tarefas trouxe agora uma enorme responsabilidade ao operador do sistema de comunicações a fim de evitar as ofensivas atuais.

1.2 Justificativa e Relevância

É de suma importância para a Marinha do Brasil e para a Estratégia Nacional de Defesa (END) que os militares conheçam os recursos de Guerra Eletrônica disponíveis nos meios que operam, bem como os de uma Força quando operando em conjunto. Por muitas vezes esse objetivo não é atingido devido à falta de interoperabilidade entre as Forças Armadas (FFAA), porém há uma batalha diária do Ministério da Defesa (MD) para que a capacitação dos recursos humanos necessários à condução da atividade de GE seja atingida (MINISTÉRIO DA DEFESA, 2004, p.13).

O avanço tecnológico tem possibilitado o uso de equipamentos cada vez mais modernos nas comunicações sem fio. E isso traz consigo um aumento de ataques contra a interceptação e alteração de mensagens transmitidas ou bloqueio de sinais, comprometendo a segurança, integridade e disponibilidade das comunicações. Tem-se então o propósito de analisar possíveis defesas para minimizar danos a segurança das comunicações e ampliar o fluxo de informações entre os meios navais.

As técnicas e procedimentos MPE ganham destaque quando os equipamentos de comunicação não podem permanecer na condição de silencio, ou seja, sem emitir.

Toda vez que se emite estará dando a oportunidade ao adversário de se obter informações através de Medidas de Apoio à Guerra Eletrônica (MAGE) e de interferir ao trânsito de por meio de Medidas de Ataque Eletrônico (MAE).

Assim sendo, em uma operação militar, tornam-se essenciais o conhecimento dos equipamentos e tecnologias de comunicações, a análise de comportamento de ondas eletromagnéticas, tendo em vista o ambiente de emprego destas, integração dos sistemas de comunicações, criptografia das mensagens e adestramento. Para que se possa de forma eficaz, empregar meios que possam anular, evitar, impedir, dificultar contra-medidas por meio de técnicas e procedimentos que serão explicitados ao longo deste trabalho.

1.3 Objetivos

As comunicações e sua proteção são essenciais para a vitória em uma batalha. O ataque, deslocamento, defesa ou qualquer ação combinada requer um nível de planejamento que deve ser transmitido aos participantes. Essa comunicação deve ser feita com antecedência e com precaução contra interceptação inimiga a fim de não se favorecerem.

Portanto, dentre os campos de atuação da GE, Não-Comunicações (NCom) e Comunicações (Com), o foco deste trabalho será neste último, com ênfase nas medidas de proteção, o qual engloba a exploração do espectro eletromagnético e equipamentos voltados ao trânsito de informações.

1.3.1 Objetivo Geral

Este trabalho realiza uma breve análise dos diferentes recursos de proteção das Comunicações e Guerra Eletrônica, apresenta, também, tecnologias nesse sentido, que possam ser requisitos para aquisição de equipamentos de comunicação.

1.3.2 Objetivos Específicos

A partir da abordagem conceitual de Guerra Eletrônica, objetiva-se explanar entendimentos fundamentais para compreensão holística do trabalho.

O conhecimento e a consciência de proteção eletrônica das comunicações nos mostra a importância de planejamento e execução das operações, aquisição de equipamentos com tecnologias inerentes e treinamento de pessoal para o sucesso das missões.

1.4 Etapas do Trabalho

O Capítulo 2 apresenta algumas considerações sobre Guerra Eletrônica e Comunicações. É feita uma abordagem inicial de conceitos de Guerra Eletrônica e onde a parte de Comunicações, que é o foco deste trabalho, se enquadra dentro do campo de Guerra Eletrônica.

O Capítulo 3 apresenta os tipos de ações que poderão ser empreendidas quando se refere a defesa electronica das comunicações. São citados tecnologias, procedimentos e cuidados que se deve ter no tratamento de informações, seleção e capacitação de pessoal.

O Capítulo 4 vai tartar sobre o referencial teórico, o qual apresenta aquilo que se pode extrair das fontes bibliográficas utilizadas para embasamento teórico deste trabalho.

O Capitulo 5 apresenta o método utilizado para pesquisa, a classificação que pode ser feita quanto ao tratamento das informações, e a dificuldade, limitação ao se explorar o assunto proposto.

Por fim, o Capítulo 6 apresenta a conclusão do trabalho, mostra as contribuições e se faz sugestões para futuros trabalhos.

2. GUERRA ELETRÔNICA E COMUNICAÇÕES

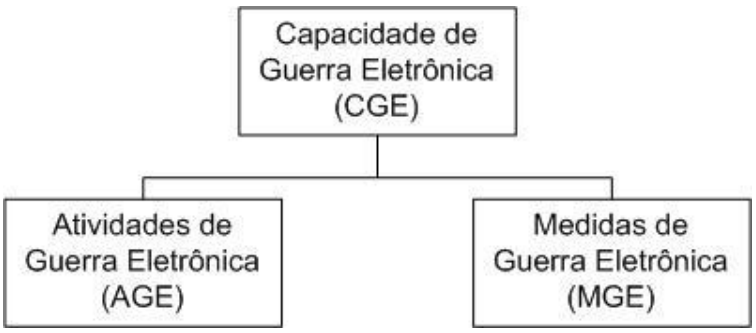
No decorrer do tempo, a guerra vem se desenvolvendo. O surgimento de novas tecnologias nos apresenta ambientes de guerra que há décadas atrás não existiam. Nesse contexto consideramos a Guerra Eletrônica.

De acordo com a Doutrina básica da Marinha (DBM) 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 (EMA, 2014, p.3).

Sua capacidade, conhecida por Capacidade de Guerra Eletrôncia (CGE), é constituída por todos os recursos necessários a uma força para pôr em prática as ações de GE. A CGE se fundamenta sob dois grupos: Atividades de Guerra Eletrônica (AGE) e Medidas de Guerra Eletrônica (MGE) - Organograma 2.1.

Organograma 2.1: Subdivisões da Capacidade de Guerra Eletrônica

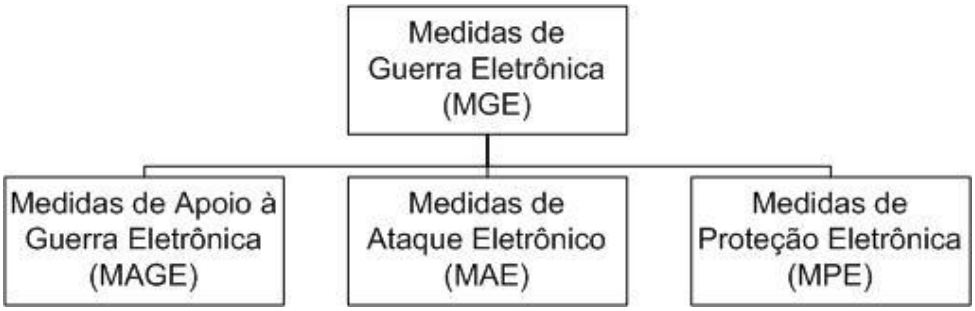


Fonte: Manual de Guerra Eletrônica

As Atividades de Guerra Eletrônica possuem uma essência estratégica e de apoio a operações de Guerra. Por outro lado, as Medidas de Guerra Eletrônica visam o emprego da CGE. E é sob este aspecto que este trabalho se desenvolverá.

Atualmente, as MGE é constituída por: Medidas de Apoio à Guerra Eletrônica (MAGE), Medidas de Ataque Eletrônico (MAE) e Medidas de Proteção Eletrônica (MPE) – Organograma 2.2.

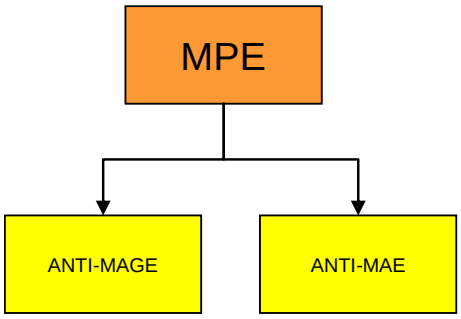
Organograma 2.2: Medidas de Guerra Eletrônica e suas subdivisões



Fonte: Manual de Guerra Eletrônica

O presente trabalho se concentra na subdivisão das Medidas de Proteção Eletrônica, com foco em Comunicações. O propósito das MPE é permitir o próprio uso do espectro eletromagnético em meio a ações contrárias com intuito de impedir, além de negar o fornecimento de informações por interceptação do sinal eletromagnético pelo inimigo. As MPE podem ser divididas de acordo com o Organograma 2.3:

Organograma 2.3: Divisões das MPE



Fonte: Manual de Guerra Eletrônica

Embora o trabalho esteja voltado para MPE, é importante conhecermos a essência das medidas que se sobrepõe aos sistemas que se pretende defender a fim de tornar essa defesa mais consciente, preditiva aos ataques, incluindo, evitar que o inimigo obtenha informações táticas e que possam colocar em risco uma operação.

A finalidade de qualquer medida de ataque eletrônico é interferir no uso efetivo do espectro eletromagnético pelo inimigo. Daí a importância de se adotar medidas de proteção eletrônica, tendo em vista que através do espectro eletromagnético são transmitidas informações que podem ser sob a forma de vídeo, voz, dados, por exemplo.

Através da inserção de um sinal interferente no receptor inimigo que concorra com o sinal desejado, tem-se o sucesso da medida de ataque eletrônico quando o sinal interferente faz com que o inimigo não consiga obter a informação de interesse. Isso pode acontecer quando o conteúdo da informação do sinal desejado se encontra saturado pelo sinal de interferência, ou se o sinal desejado acrescido do sinal de interferência apresentar características tais que impeçam o analista inimigo de obter a informação adequada do sinal.

Sendo assim, as Medidas de Ataque Eletrônico para sistemas de comunicação são, basicamente, a inserção de interferências sobre o enlace de comunicações.

Enquanto que as Medidas de Apoio à Guerra Eletrônica, que possuem uma natureza passiva, visam, fundamentalmente, fornecer dados e informações à coordenação ou comando para apoiar o processo de decisão em meio a uma operação; pois serão úteis para avaliação de ameaças e orientação de emprego de ações de MAE.

Portanto, serão abordadas ações anti-MAE e anti-MAGE, conforme o propósito e as subdivisões da MPE.

3. MEDIDAS DE PROTEÇÃO ELETRÔNICA

3.1 Procedimentos de Medidas de Proteção Eletrônica

Tem por objetivo elevar o grau de confiabilidade e segurança das emissões, além de impedir ou dificultar o emprego das MAGE e MAE pelo oponente.

3.1.1 Mudança de Frequência – Anti-MAGE

Caso o equipamento não possua a tecnologia que permita a variação de frequência automaticamente, salto de frequência, por exemplo. Constitui uma MPE a mudança manual de frequência em intervalos de tempos não uniformes, ou seja, que não sigam um padrão facilmente detectável, por exemplo: de 8 em 8 minutos. Porque isto facilita o análise do inimigo que poderá prever a próxima troca de frequência. Recomenda-se que as frequências a serem utilizadas possam estar descritas em um caderno de instruções, e observar, sempre que possível, a existência de frequências reservas.

Destaca-se a relevância de se separar frequências de operação para uso em guerra, situação real, e, assim, mascarar a totalidade dessas frequências a inteligência inimiga.

3.1.2 Mudança de Frequência – Anti-MAE

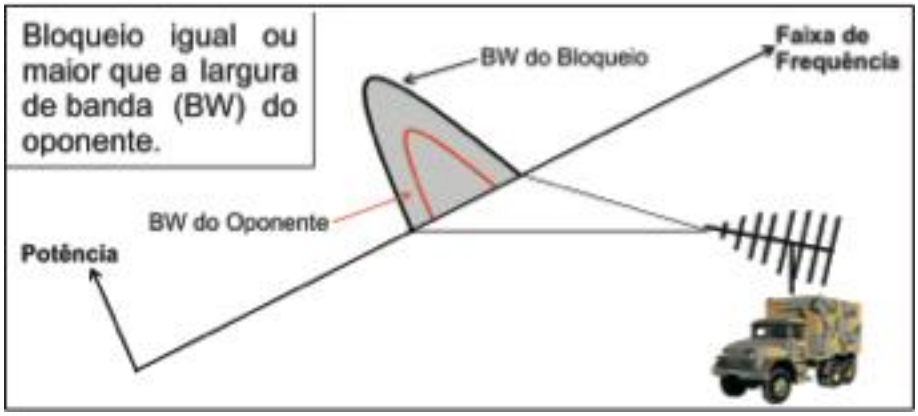
Considera-se a força amiga sujeita a uma MAE não-destrutiva, ou seja, que não causa prejuízo físico ao inimigo. Exemplifica-se a de bloqueio de ponto. Nesta MAE, após a obtenção da frequência de operação adversária pelo MAGE, concentra-se a energia em uma estreita faixa de frequência sobre a largura de banda ocupada pelo espectro do receptor inimigo. Assim, impede ou degrada a sua recepção e análise do sinal.

É importante destacar diante dessa situação, que ao se identificar qualquer ação de bloqueio, deve-se trocar a frequência. Porém, é de suma importância que esta troca seja feita cuidadosamente a fim de que não seja notada pelo agente ofensor, pois estará explicitando a eficácia da MAE e, assim, a ação poderá ser intensificada pelo inimigo.

Uma forma de dissimular o efeito de uma MAE bem sucedida é: quando a MAE for identificada durante a transmissão de uma mensagem, esta deve ser transmitida até o fim. Então se aguarda a hora de mudança pré-programada de frequência ou se altera a frequência por meio de mensagem previamente estabelecida.

Caso o equipamento não permita uma diversidade de frequência de operação, outra opção seria a utilização de um equipamento diverso, que execute a mesma função do primeiro, porém com parâmetros de irradiação diferentes.

Figura 3.1: Bloqueio de ponto



Fonte: BRASIL(2007)

3.1.3 Mudança de Indicativo – Anti-MAGE

Dificulta a Análise de Tráfego, ainda mais quando desassociado à mudança de frequência. Pois, quando em mesma frequência, o inimigo pode ser induzido a pensar que há outro elemento ativo na rede.

Melhora a eficácia dessa medida se houver mudança de operadores, neste caso em redes-rádio.

3.1.4 Autenticação de Posto – Anti-MAE (Despistamento)

Autenticação consiste em uma medida de segurança que visa a proteção dos sistemas de comunicação contra transmissão ou mensagens falsas introduzidas pelo inimigo com o propósito de induzir a ações erradas, confundir ou descobrir conteúdo de mensagens importantes. De forma mais específica, a autenticação de posto tem o intuito de verificar se o posto transmissor ou receptor pertence a força amiga.

Sendo assim, será solicitada a autenticação do posto quando houver desconfiança de uma ação de Despistamento Imitativo, MAE que consiste em disseminar uma mensagem falsa na rede. Portanto, a Autenticação do Posto poderá seguir uma norma do tipo “senha e resposta” em que o agente da MAE irá corresponder de forma incorreta.

São fatores que motivam a Autenticação do Posto:

a) ordem na rede que fuja dos padrões de mensagens que estavam sendo transmitidas;
b) ordens de deslocamento do meio operativo fora do contexto previsto da operação;
c) ordens que solicitem informações sobre a operação, por exemplo: nome das unidades, posições dos meios ou tropas, efetivo;
d) radioperador desconfiar da voz do seu interlocutor;
e) uma estação rádio entra na rede;
f) mensagens são transmitidas em claro;
g) houver instruções para mudança de frequência ou disseminação de contatos não obstante tais ações terem sido realizadas;
h) é feito uma transmissão a uma estação que esteja em silêncio;
i) houver estabelecimento ou encerramento de uma condição de silêncio rádio; e
j) sempre que houver suspeitas a respeito da autenticidade de uma transmissão.

3.1.5 Mudança de Posição – Anti-MAGE/Anti-MAE

A mudança da posição de uma antena ou posto-rádio traz por consequência uma alteração no alcance de transmissão. E isso influencia tanto a recepção MAGE da força oponente quanto a recepção MAE inimiga.

Todavia, uma mudança de posição de um ou mais meios operativos deve ser planejado e coordenado, pois implicará em possíveis mudanças na derrota, formaturas ou atrasos de chegada. Também se considera a manutenção do mínimo enlace de comunicação de forma que não se perca totalmente a comunicação com os demais meios.

3.1.6 Aproveitamento do Terreno – Anti-MAGE/Anti-MAE

Considera-se, ao alterar a posição de uma antena ou estação, a existência de obstáculos no terreno que dificultem as ações de MAGE e/ou MAE inimigas. São exemplos de obstáculos que podem influenciar estas ações em um ambiente terrestre: edifícios, linhas de alta tensão, matas densas ou florestas, espelhos d'água. É recomendável que as posições adotadas sejam, se possível, de forma que o obstáculo esteja entre a estação e a emissão do inimigo, pois assim a onda eletromagnética fica passiva de fenômenos de reflexão, absorção e refração.

De fato, a técnica de aproveitamento de terreno usa, em parte, o bloqueio mecânico como medida de proteção. Pois, por definição, o bloqueio mecânico consiste em aproveitar meios físicos para refletir a EEM inimiga para diminuir a sua capacidade de detecção. Um exemplo seria o Chaff.

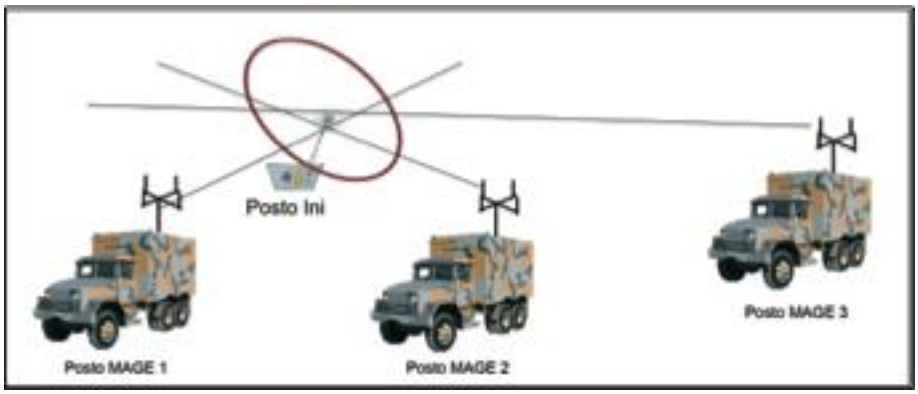
3.1.7 Antenas Direcionais – Anti-MAGE/Anti-MAE

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 3.2: Localização horizontal



Fonte: BRASIL(2007)

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

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

3.1.8 Mensagem Preestabelecida – Anti-MAGE

Desta técnica podemos depreender dois pontos, o primeiro diz respeito a interceptação da mensagem transmitida pelo inimigo. Exemplificamos da seguinte forma, suponha que o inimigo intercepte a seguinte mensagem: “F43 abrir fogo ao UJ 1401”, o adversário pode interpretar o comando. Todavia, se esta mensagem fosse substituída por: “SOL BRILHANDO EM MARTE”, haveria um grau maior de dificuldade por parte do oponente para prever as consequências dessa mensagem de forma rápida, ao menos que ele tivesse as instruções do exercício em andamento.

Porém, ao longo da operação, o analista pode conseguir correlacionar as mensagens aos comandos executados. Sugere-se, então, uma troca periódica dessas instruções.

A segunda observação relevante a este tipo de técnica é a correta interpretação da mensagem pela força amiga. Para isso, é necessário a previsão de erros nessa interpretação e o estabelecimento de adestramento do pessoal.

A prática; tanto deste procedimento de Mensagem Preestabelecida quanto do procedimento de Códigos de Nomes que será exposto no tópico a seguir; objetiva um obstáculo ao operador ou analista inimigo ao que tange à análise imediata, que é aquela realizada logo após o contato com o sinal emitido. Este obstáculo gera um atraso ao inimigo quanto ao estabelecimento de nível de interesse do sinal, identificação de ameaças, classificação de prioridade de alvos disponíveis.

3.1.9 Códigos de Nomes – Anti-MAGE

Atribuindo um código ou nome a um comando, através da combinação desses nomes, há possibilidade de maior quantidade de variações de mensagens se comparado a técnica de mensagem preestabelecida.

A seguinte situação pode ser considerada, para uma frase preestabelecida, há uma correspondente interpretação. Por exemplo, se receber “SOL BRILHANDO EM MARTE”, leia “F43 abrir fogo ao UJ 1401”. Ao passo que, se criarmos uma tabela com cada nome correspondendo a uma ação, podemos combinar os nomes e criar comandos diferentes.

Quadro 3.3: Código de nomes

CÓDIGO	**SITUAÇÃO**
SOL	F43
LUA	F41
BRILHANDO	ABRIR FOGO
NUBLADO	ENTRAR EM FORMATURA
EM MARTE	UJ 1401
NA CAVERNA	FORM D

Fonte: O Autor

3.1.10 Controle de Potência – Anti-MAGE/Anti-MAE

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

Deve-se atentar ao fato de que uma potencia mais baixa do que o necessário para se comunicar, desvia a finalidade de se estabelecer a comunicação e se torna uma vitória da MAE inimiga.

Entretanto, quando a força amiga está sofrendo uma ação de bloqueio, temos que o aumento da potencia pode transpor essa ação, constituindo, assim, uma medida Anti-MAE.

Embora a constatação de um aumento do nível de potencia pelo inimigo seja percebido através da potencia recebida, isso não é suficiente para o ofensor concluir que a ação de bloqueio empregada foi eficaz.

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

3.1.11 Uso de repetidores e retransmissores – Anti-MAGE/Anti-MAE

Encurta a distancia de transmissão entre estações. Consequência disso é a diminuição da potencia de transmissão e mais consistência nos enlaces de comunicação.

Assim sendo, trata-se de um recurso que visa reduzir as ações MAE e/ou MAGE inimiga.

3.1.12 Mudança de Polarização – Anti-MAGE/Anti-MAE

Polarizações defasadas de 90º ocasionam enormes perdas de sinais (ver quadro 3.4). É extremamente relevante que as antenas de transmissão entre duas estações que se desejam comunicar estejam com a mesma polarização. Este mesmo fundamento é utilizado pela antena de MAGE em relação ao emissor de interesse.

Altera-se a polarização de uma antena pela troca da antena, por exemplo. Outra opção seria alterar a inclinação de uma antena vertical em 90º e, desta forma, ela passa a se comportar semelhantemente a uma antena com polarização horizontal, com características, inclusive, de diretividade. Neste caso, é preciso direcionar a antena na marcação correta da estação a qual se deseja comunicar.

Assim sendo, pode-se utilizar esse recurso de mudança de polarização quando se estiver passivo de MAE, ou para evitar interceptação por MAGE, por exemplo.

O quadro 3.4 demonstra o impacto da polarização conforme algumas combinações de antenas de transmissão e recepção selecionadas.

Quadro 3.4 – Perda de polarização da antena

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

Fonte: Adaptado de Electronic Warfare Fundamentals

3.1.13 Mudança do Tipo de Modulação e/ou Protocolo de Transmissão

A alteração no tipo de modulação (exemplos de modulação) e protocolo (exemplos de protocolos) na transmissão de mensagens cria um enorme obstáculo ao inimigo que interceptar uma transmissão, pois este teria de ser capaz de decodificar e demodular o sinal, caso tenha tecnologia para o fazer. E ainda que o tenha, mudanças periódicas na modulação e demodulação são técnicas que podem dar mais trabalho ao inimigo para análise e interpretação do sinal.

Se a força inimiga não tiver tecnologia para decodificar e demodular o sinal interceptado, a possibilidade se torna mínima de se obter a informação deste sinal.

3.2 Tecnologias de Medidas de Proteção Eletrônica

Segundo Spezio (2002) o domínio do EEM possui papel de extrema importância nos conflitos mundiais e o uso de tecnologia que proporciona o controle deste permite definir a vitória ou a derrota em um conflito militar.

Considerando isso, serão apresentadas tecnologias utilizadas nos sistemas eletrônicos pela força amiga com o propósito de proteção as Comunicações contra MAGE ou MAE oponentes.

3.2.1 Salto de Frequência – Anti-MAGE/Anti-MAE

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, p.310).

Presente em equipamentos mais modernos, é fundamental que na execução desta técnica as estações estejam sincronizadas quanto as mudanças de frequência.

Existe bloqueio em sistemas com salto em frequência. Para isso, também há um anti-bloqueio.

Pode-se supor uma situação em que o salto em frequência seja rápido de tal forma que o bloqueio não consiga cobrir a mesma faixa do espectro de frequência do sinal a ser bloqueado. Tem-se, então, que o bloqueio não se torna eficaz. Exemplificamos esta situação da seguinte forma: seja um sistema a emitir em uma frequência f1, após alguns segundos o bloqueador emite o seu sinal na mesma frequência f1. Entretanto, pelo tempo de resposta do bloqueador, o sistema já saltou para uma frequência f2, fazendo com que o bloqueio perca a eficiência.

3.2.2 Criptofonia – Anti-MAGE

Consiste em embaralhar o sinal de mensagem pré-transmissão. Para interpretar a mensagem transmitida, é preciso que o receptor tenha a chave criptográfica. Por este motivo 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.

3.2.3 Controle automático de Potência – Anti-MAGE/Anti-MAE

Consiste em ajustar a potencia de transmissão a um nível mínimo suficiente para se estabelecer a comunicação.

É uma ação anti-MAGE, pois trará maiores dificuldades ao inimigo para interceptar um sinal de baixa potencia.

Por outro lado, considera-se uma ação anti-MAE porque, quando a estação receptora estiver sofrendo uma ação de bloqueio, o transmissor pode responder aumentando a potencia de transmissão.

3.2.4 Criptografia – Anti-MAGE

Essa técnica é baseada em codificar a informação ou a tornar ininteligível de forma que somente os destinatários autorizados possam acessar o conteúdo, decodificar a informação. Normalmente são utilizadas chaves para criptografar. Estas chaves são divididas em: assimétricas e simétricas.

Criptografia com chave simétrica é utilizada uma única chave tanto para criptografar como para decriptografar. Porém essa técnica tem a vulnerabilidade caso se descubra a senha, pois permitirá o acesso a informação.

Já a criptografia com chave assimétrica são utilizadas chaves diferentes para criptografar e decriptografar, garantindo, assim, com maior confiança a autenticidade e não-repúdio a mensagem.

3.2.5 Esteganografia – Anti-MAGE/Anti-MAE

Considerando 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.

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.

3.2.6 Transmissão por salvas (BURST) – Anti-MAGE

Possibilita ao rádio a compressão da mensagem. Caso esta seja grande, ela será dividida em pacotes, desde que não haja a transmissão de outra mensagem entre os intervalos de transmissão da primeira.

Tal técnica evitará a localização eletrônica e interceptação.

3.2.7 Transmissão digital de voz – Anti-MAGE

Com intuito de tornar a comunicação mais eficaz, essa tecnologia traz mais confiança a comunicação e a deixa menos vulnerável a ruídos.

Considerada uma medida anti-MAGE porque poucos sistemas MAGE possuem tecnologia suficiente para acessar o conteúdo da informação digital de voz transmitida.

3.3 Procedimentos de Segurança das Comunicações

3.3.1 Introdução

É comum que as pessoas tenham mais cuidado se a mensagem for explicitamente sigilosa. O problema é quando um grande volume de mensagens, aparentemente isoladas ou não sigilosas, são transmitidas indiscriminadamente e, se analisadas em conjunto, fornecem conteúdo restrito.

Uma opção para segurança na transmissão é o uso de criptografia, entretanto, devido a conveniência de rapidez na transmissão, não raro se usa canais rádio muito suscetíveis a interceptação ou mesmo sem criptografia. Observa-se em todo tempo a busca pelo equilíbrio entre segurança e rapidez.

O inimigo tenta de várias formas obter informações. Sabe-se que as investidas nas comunicações podem ocorrer pela interceptação de tráfego rádio, obtenção de códigos e cifras, estabelecimento de espião em centros de comunicação, interceptação de comunicação telefônica, mensagens e até mensageiros.

3.3.2 Medidas preventivas

A fim de evitar o sucesso inimigo, algumas medidas podem ser adotadas. Dentre elas, podemos destacar a seleção de pessoal com características evidenciadas e positivas de caráter, lealdade e discrição; a escolha de locais seguros para tratamento de materiais sigilosos como locais de maior vigilância quanto ao acesso por pessoas não autorizadas, além de se adotar o registro de movimentação do material; existência de um plano de destruição do material sigiloso de comunicações quando em iminência de obtenção pela força oponente; medidas para preservação, controle e acesso ao material sigiloso tais quais a escrituração, distribuição, embalagem.

3.3.3 Exploração

Há basicamente duas formas de se explorar as comunicações adversárias: interceptação e intromissão por imitação. Esta consiste em escutar ou gravar informações destinadas a outrem. Aquela pela introdução nos canais de comunicação de transmissões despistativas, com o propósito de confundir ou influenciar as interpretações do conteúdo das mensagens ou penetrar nas redes. Contra esses ataques, podemos adotar medidas de segurança para o emprego rádio, disciplina rádio e na transmissão sem fio.

A atribuição de graus de restrição ao emprego de rádio pode ser:

a. silencio absoluto: transmissores e receptores desligados;
b. silencio: somente receptores ligado;
c. restrito: somente transmissão de mensagens urgentes; e
d. livre: transmissão e recepção livres.

A percepção, entretanto, de restrições pelo oponente pode levá-lo a dedução de uma operação importante em curso. Por isso a importância de se manter um volume constante de mensagens.

A manutenção da disciplina rádio implica em utilizar nas comunicações as regras de exploração em vigor, ou seja, o correto grau de restrição; eliminar as transmissões desnecessárias, para isso, recomenda-se pensar bem no que vai ser transmitido antes de fazer uma chamada; escutar antes de transmitir, clareza e precisão ao falar e brevidade ao responder, e observar, na transmissão para mais de um posto, a cadência do operador mais fraco; e estabelecimento de postos falsos.

Além disso, considerando uma transmissão sem fio, não se deve negligenciar o controle do pessoal que opera na central, participar imediatamente a ocorrência de ruídos suspeitos e, ao término de uma conversação, dar o sinal de fim.

3.3.4 Treinamento de pessoal

Os usuários dos equipamentos de comunicação devem estar familiarizados com o alfabeto fonético internacional (ver Anexos A e B). O emissor de uma mensagem de voz deve ter cadencia ao falar, clareza, concisão. Porque se acontecer de o receptor não compreender a mensagem e solicitar a repetição, dará chance ao inimigo de mais uma vez interceptar a transmissão.

Evitar termos ou palavras parecidas foneticamente, porém com significados diferentes.

Manter o botão PTT (push to talk) pressionado por muito tempo, assim dificulta a interceptação e localização eletrônica.

Canal de coordenação da rede diferente do canal de comunicação.

Evitar ruído de fundo, conversas, durante a transmissão. Transmitir somente o necessário.

O conhecimento de mensagens pré-estabelecidas a partir de associação palavra-código, substitui o uso direto de informações táticas como lugar, posição, designação de OM (Organização Militar), horário. Ao militar envolvido na comunicação por este método deve estar treinado para fazer a associação correta, hábil e clara ao transmitir ou interpretar o conteúdo da mensagem.

4. REFERENCIAL TEÓRICO

O Manual de Guerra Eletrônica e o livro de Electronic Warfare Fundamentals apresentam informações conceituais de elevado valor ao se tratar de todas as ações no campo da Guerra Eletrônica.

A publicação da marinha DGMM-0540 traz o balizamento importante sobre as atividades correlatas a política de segurança das comunicações da Marinha do Brasil.

Da dissertação Silva (2009), podemos extrair exemplos de técnicas de bloqueio, além de acrescentar conceitos sobre GE.

Somados a essas fontes, temos os Manuais de Campanha do Exército que vão ampliar os conceitos e, principalmente, técnicas aplicadas à GE. Também complementará as normas de Segurança das Comunicações.

5. METODOLOGIA

Materiais ministrados em sala de aula indicaram a base de pesquisa para o desenvolvimento deste trabalho, além de entrevistas com Oficiais Comunicativos embarcados.

Foram feitas pesquisas em sítios da internet de arquivos voltados para assuntos militares. Publicações existentes ajudaram a entender elementos conceituais.

Análise de tecnologias e procedimentos utilizados por aqueles que operam com equipamentos e centros de comunicações através de publicações, exemplificam e dimensionam as ameaças e necessidade de um conhecimento sólido sobre medidas de

proteção eletrônica. E pesquisas bibliográficas com a apresentação de teses ampliam o horizonte de conhecimento.

5.1 Classificação da Pesquisa

Aplica-se um método descritivo para este trabalho, em sua maioria. Com exposições de características de recursos empregados, realizando análises e sugestões de tecnologias e ações manuais e naturais para as diversas situações operacionais em um ambiente complexo que envolve comunicações em guerra eletrônica.

Há, também, um caráter explicativo, pois após a exposição de recursos e métodos aplicados, busca-se apresentar uma breve explanação e levar ao entendimento do porquê da utilização destes.

5.1.1 Quanto aos fins

Com a finalidade de se atingir o objetivo geral, explicita-se possíveis linhas de ações aplicáveis ao presente e passíveis de um aprimoramento futuro, seja no desenvolvimento material seja no pessoal.

5.1.2 Quanto aos meios

Fundamentalmente bibliográfica e documental. Aquela porque grande parte do referencial teórico deriva de artigos, teses e publicações relativos ao problema abordado. Trata-se de pesquisas na área de sistema estratégico de GE, que trazem conceitos essenciais para o desenvolvimento desse trabalho.

Documental pois são publicações, algumas da Marinha do Brasil (MB), outras do Exército Brasileiro (EB), que mostram as características operativas dos diversos equipamentos utilizados nos meios empregados e táticas furtivas e preventivas aplicadas ao adestramento de pessoal.

5.2 Limitações do Método

Observa-se, após levantamento da literatura sobre o assunto, que há pouca disponibilidade ostensiva de artigos, livros e trabalhos, o que dificultou em certa maneira o desenvolvimento do trabalho.

Ao se tratar de Guerra Eletrônica nas Comunicações, pode-se imaginar a dificuldade em se apresentar métodos empregados por outras forças armadas, pois, mesmo em tempos de paz, procura-se a todo momento a formação de uma biblioteca de informações e características de equipamentos e emissão (frequência, modulação, frequência de repetição de pulsos – FRP, cifras, códigos, chaves, entre outras características) para em tempos de guerra identificar, atacar e defender.

Portanto, esgotar os procedimentos, bem como, elencar todas as tecnologias existentes se torna um grande desafio, e afirmar esse conhecimento não teria uma precisão matemática.

Assim sendo, buscou-se exemplificar métodos empregados, principalmente, pelas FFAA brasileiras. Incluindo treinamento ou sugestões de treinamentos que possam diminuir uma possível defasagem tecnológica.

5.3 Coleta e Tratamento de Dados

Publicações trazem uma bagagem conceitual fundamental para entendimento inicial de assuntos que virão posteriormente.

Pesquisas de artigos e matérias mostram a necessidade de se ter uma mentalidade para uma guerra tecnológica em que ofensivas são, a princípio, imperceptíveis, porém suas consequências são enormes, desastrosas e bem visíveis. Assim, o trabalho se desenvolve, após uma abordagem conceitual, com técnicas de proteção.

Teses e trabalhos acadêmicos ajudam a compor o corpo do trabalho com exemplos de equipamentos, tecnologias e ações utilizadas em um meio eletromagneticamente hostil, bem como auxiliar a formulação de medidas de prevenção e resiliência.

6. CONCLUSÃO

O trabalho abordou teoricamente as técnicas de proteção eletrônica utilizadas pelos sistemas de comunicações. Foram apresentados procedimentos, condutas ou métodos

que podem ser adotados pelos militares face a ausência de algum recurso tecnológico diante da percepção de um ataque eletrônico e, inclusive, para se evitar tais ataques.

Para equipamentos mais modernos de comunicação, foram apresentados tecnologias inerentes que dificultam a interceptação da informação pelo inimigo e a inserção de ruídos na recepção do sinal que por vezes atrasa ou até mesmo impede a interpretação dos dados.

Foi vislumbrado o quão é importante o papel daqueles envolvidos no processo de comunicação e foi necessário que este trabalho destacasse que os usuários devem estar aptos a utilizarem as tecnologias constantes nos equipamentos, e bem adestrados para se colocar em prática os procedimentos de forma correta. A melhor forma de se contrapor a uma MAE é a precisa utilização de métodos Anti-MAGE e o emprego preciso de MPE, rápido e consciente.

Nem todas as técnicas foram abordadas neste trabalho, mas consideremos a relevância de se treinar, adestrar o pessoal, a realização de exercícios antes de operações reais. Para explorarem melhor os recursos disponíveis e não comprometerem a segurança das informações por falta de coordenação ou habilidade na execução dos procedimentos.

Portanto, buscou-se contribuir para o fortalecimento de conhecimentos na área de medidas de proteção eletrônica com ênfase em comunicações uma vez que se observa na Marinha do Brasil um grande foco para ações contra radares. É de salientar ainda que o caráter exploratório deste trabalho voltado para tais medidas atingiu o objetivo de despertar uma consciência maior sobre o tema, demanda por tecnologias de proteção e, não obstante, o desenvolvimento posterior de doutrinas mais amplas sobre o assunto.

6.1 Sugestões para Futuros Trabalhos

Torna-se um ato ousado tentar esgotar um estudo de ações, procedimentos e tecnologias, de proteção eletrônica das comunicações face as novidades de exploração do espectro eletromagnético as quais se desenvolvem com relação direta ao avanço tecnológico com o propósito de confundir, evitar, anular ou interceptar o fluxo de informações e sua interpretação.

Então, o estudo dessas ações voltadas as medidas de proteção eletrônica em pesquisas futuras seria de estrema relevância para o aumento de nossa capacidade operativa de se comunicar com segurança.

Outrossim, estudos voltados para uma formação mais específica, com incremento de matérias nos cursos, no campo de Guerra Eletrônica de Comunicações aliado a parte prática de fonia e elaboração de exercícios, simulando, inclusive, a operação conjunta com forças internacionais seriam bastante oportuno. E contribuiriam para uma formulação de fontes maiores de doutrinas de Guerra Eletrônica de Comunicações e até um possível surgimento de organizações militares dedicadas exclusivamente para esse setor.

REFERÊNCIAS

ALFABETO Fonético, Código Q, OTAN e Internacional: **Alfabeto fonético da OTAN**. Disponível em: <http://www.oarquivo.com.br/variedades/ciencia-e-tecnologia/4197-alfabeto-fon%C3%A9tico,-c%C3%B3digo-q,-otan-e-interncacional.html>. Acesso em: 22 maio 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.

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

Electronic Warfare Fundamentals, November 2000, 351 p.

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

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.

SILVA, Alex Alvarez da. **Simulação e Análise da Eficácia das Técnicas de Bloqueio em Sistemas de Comunicações**: Ênfase no Sistema GSM. 2009. 142 f. Dissertação (Mestrado) – Curso de 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, mar. 2002. Disponível em: <http://ieeexplore.ieee.org/document/989948/>. Acesso em 21 Jan. 2018.

GLOSSÁRIO

Antenas Direcionais - São as que maximizam a irradiação numa determinada direção e minimizam a recepção e a irradiação nas outras direções.

Bloqueio - É a irradiação intencional, reirradiação ou reflexão de energia eletromagnética com a finalidade de reduzir ou anular a recepção do sinal dos equipamentos ou sistemas eletrônicos/eletroópticos em uso pelo oponente.

"Chaff" - O "Chaff" é composto por pequenas tiras ou fios de metal, de plástico ou fibra de vidro metalizados, que têm a finalidade de agir como refletores, fornecendo autoproteção contra radares.

Guerra Eletrônica (GE) - É o conjunto de atividades que visam desenvolver e assegurar a capacidade de emprego eficiente das emissões eletromagnéticas próprias, ao mesmo tempo em que buscam impedir, dificultar ou tirar proveito das emissões inimigas.

Localização Eletrônica - Consiste na determinação da área provável do emissor-alvo de sinais eletromagnéticos por meios eletrônicos (receptores, processadores e sistemas especiais de antenas).

Medidas de Apoio de Guerra Eletrônica (MAGE) - Objetivam a coleta de dados e informações a partir das emissões eletromagnéticas do oponente.

Medidas de Ataque Eletrônico (MAE) - Caracterizam-se pelas ações executa- das para impedir ou reduzir o uso efetivo do espectro eletromagnético pelo inimigo, bem como destruir, neutralizar ou degradar sua capacidade de combate, usando energia eletromagnética ou armamento que empregue a emissão do alvo para o guiamento.

Medidas de Proteção Eletrônica (MPE) - São as ações executadas para assegurar o uso efetivo do espectro eletromagnético, a despeito das ações de GE ou interferências.

ANEXO A – Alfabeto Fonético Da Otan (Letras)

Letras

Letra	Código	Pronúncia em todas as línguas
A	**alfa**	**al** fa
B	**bravo**	**bra** vo
C	**charlie**	**tchar** li
D	**delta**	**del** ta
E	**echo**	**é** cô
F	**foxtrot**	**fox** trot
G	**golf**	**golf**
H	**hotel**	ho **tel**
I	**indi**a	**in** dî a
J	**juliett**	**djou** li ett
K	**kilo**	**qui** lô
L	**lima**	**li** ma
M	**mike**	maic
N	**november**	no **vem** ber
O	**oscar**	**oss** car
P	**papa**	pa **pa**
Q	**quebec**	qué **bec**
R	**romeo**	**ro** me ô
S	**sierra**	si **e** rra
T	**tango**	**tan** gô
U	**uniform**	**iu** ni form
V	**victor**	**vic** tor
W	**whiskey**	**uîs** qui
X	**x-ray**	**ecs** rei
Y	**yankee**	**ian** qui
Z	**zulu**	**zu** lu

Fonte: www.oarquivo.com.br

ANEXO B – Alfabeto Fonético da Otan (Números)

NO BRASIL		
Número	**Código**	**Pronúncia em português Brasileiro**
0	Zero	**zé** ro
1	Um	**Um**
2	Dois	**Dois**
3	Três	**Três**
4	quatro	**qua** tro
5	cinco	**cin** co
6	Meia	**mei** a
7	Sete	**sé** te
8	Oito	**oi** to
9	Nove	**nó** ve

Fonte: www.oarquivo.com.br