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

EMPREGO DA GUERRA ELETRÔNICA PARA SUBSIDIAR AS AÇÕES DE COMANDO E CONTROLE

1°Ten EVERTON JULIO DOS SANTOS COSTA

Rio de Janeiro
2021

1°Ten EVERTON JULIO DOS SANTOS COSTA

EMPREGO DA GUERRA ELETRÔNICA PARA SUBSIDIAR AS AÇÕES DE COMANDO E CONTROLE

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

Orientadores:
Capitão - Tenente Bruno Siqueira Ferreira
Capitão - Tenente Danilo Caldas Marinho

CIAW
Rio de Janeiro
2021

FOLHA DE APROVAÇÃO

1°Ten EVERTON JULIO DOS SANTOS COSTA

EMPREGO DA GUERRA ELETRÔNICA PARA SUBSIDIAR AS AÇÕES DE COMANDO E CONTROLE

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:

Capitão – Tenente Bruno Siqueira Ferreira – NDCCMMaia _____

Capitão – Tenente Danilo Caldas Marinho – NVAratu _____

Juarez da Silveira Figueirêdo, MSc – PUC Rio _____

CIAW
Rio de Janeiro
2021

AGRADECIMENTOS

A Deus, pela saúde e disposição que tem me concedido para transpor as dificuldades.
À minha mãe, Ediza, que durante toda minha vida tem sido o meu maior exemplo.
À minha esposa, Daiana, por todo carinho, amor diário e apoio incondicional.
À minha filha, Helena, por ser o amor da minha vida e me fazer ser um homem melhor.
Ao meu tio, David, por todo apoio e camaradagem durante toda a minha vida.
Ao meu primo, Cleiton, por todo carinho e afeto.
Aos meus orientadores, CT Bruno Siqueira e CT Danilo Marinho, pela disponibilidade, autonomia e apoio prestado.
A todos os professores, instrutores e coordenadores que colaboraram direta ou indiretamente para que eu lograsse êxito na execução do curso.

“O homem não teria alcançado o possível se,
repetidas vezes, não tivesse tentado o impossível”
Max Weber

EMPREGO DA GUERRA ELETRÔNICA PARA SUBSIDIAR AS AÇÕES DE COMANDO E CONTROLE

Resumo

Neste trabalho será apresentado a importância que um Comandante possui durante uma operação militar, baseado no seu poder decisório. A atuação de um líder diante dos seus subordinados é empregada através do que é chamado de Comando e Controle (C^2). A aplicabilidade do C^2 tem aumentado de forma exponencial nos últimos anos e vem se destacando devido à sua grande relevância nas guerras modernas, tendo como apoio a Guerra Eletrônica (GE). O emprego da tecnologia da informação faz com que as operações de guerra possam se desenrolar de forma eficaz, mantendo o nível de trabalho do comando, mas favorecendo exponencialmente o aumento de ameaças e recursos aplicáveis durante as operações de guerra. O objetivo Geral deste trabalho consiste na análise e na conceituação das vertentes que envolvem a GE e o C^2. A Metodologia empregada consiste em uma revisão bibliográfica, sendo empregada através de questões norteadoras e critérios de inclusão e exclusão, onde foram selecionados uma gama de publicações para compor a revisão, sendo estas selecionadas através do Google Acadêmico, *Naval Postgraduate school* e Scielo. Como resultante da pesquisa, foi elaborado uma análise *Swot* apresentando as forças, as fraquezas, as oportunidades e as ameaças conforme a abordagem e a temática apresentadas, bem como o conhecimento sobre os equipamentos empregados atualmente e as perspectivas futuras, como exemplo, o MAGE MK3.

Palavras- chave: Guerra Eletrônica. MAGE. Marinha do Brasil. Comando e Controle, Informação. Sistema Naval.

LISTA DE FIGURAS

Figura 2.1: Interações eletromagnéticas 13
Figura 2.2: Divisão da Capacidade de Guerra Eletrônica (CGE) 15
Figura 2.3: Ações básicas da AGE 16
Figura 2.4: Organograma da MGE 17
Figura 2.5: Parâmetros medidos pelo sistema MAGE 17
Figura 2.6: Medidas de Ataque Eletrônico 18
Figura 2.7: Ciclo de OODA 20
Figura 2.8: Estação Fixa do SISCOMIS 23
Figura 2.9: Área de cobertura satelital do SISCOMIS 24
Figura 2.10: Recursos do SISCOMIS 24
Figura 2.11: Croqui do MAGE MK3 das FCT. 32

LISTA DE TABELAS

Tabela 2.1: Correlação entre GE e C^2 30
Tabela 2.2: Aspectos do DEFENSOR 30
Tabela 4.1: Análise *Swot* 35

LISTAS DE SIGLAS E ABREVIATURAS

AGE	Atividades de Guerra Eletrônica
APEL	Aprestamento Eletrônico
C^2	Comando e Controle
CASNAV	Centro de Análises de Sistemas Navais
CGE	Capacidade de Guerra Eletrônica
COMTOM	Comandante do Teatro de Operações Marítimas
EEM	Espectro Eletromagnético
ELINT	Inteligência Eletrônica
FCT	Fragata Classe Tamandaré
GE	Guerra Eletrônica
IIGM	Segunda Guerra Mundial
INTCOM	Inteligência de Comunicações
IOL	Interface com operador
HF	Alta Frequência
MAE	Medidas de Ataque Eletrônico
MAGE	Medidas de Apoio à Guerra Eletrônica
MGE	Medidas de Guerra Eletrônica
MPE	Medidas de Proteção Eletrônica
RECIM	Rede de Comunicação Integrada da Marinha
RETRON	Reconhecimento Eletrônico
SISCOMIS	Sistema de Comunicações Militares por Satélite
$SISNC^2$	Sistema Naval de Comando de Controle
SWOT	*Strengths, Weaknessess, Opportunities and Threats*
TI	Tecnologia da Informação
UP	Unidade de Processamento

SUMÁRIO

1 INTRODUÇÃO 11
1.1 Apresentação do Problema 11
1.2 Justificativa e Relevância 11
1.3 Objetivos 12
1.3.1 Objetivo Geral 12
1.3.2 Objetivos Específicos 12

2 REVISÃO BIBLIOGRÁFICA 12
2.1 Guerra Eletrônica 13
2.1.1 Capacidade de Guerra Eletrônica 14
2.2 Comando e Controle 19
2.2.1 Conceituação de Comando e Controle 19
2.2.2 Sistema Naval de Comando e Controle 22
2.2.3 Satélite de Comunicação e sua aplicabilidade no SISCOMIS 23
2.2.4 Importância da Informação 25
2.2.5 A Guerra de Comando e Controle 25
2.3 Guerra Eletrônica x Comando e Controle 26
2.3.1 MAGE e Inteligência de Sinal 27
2.3.2 MAE 28
2.3.3 MPE 28
2.3.4 Breves considerações sobre a GE como auxílio para o C^2 29
2.4 Equipamentos empregados no auxílio ao C^2 30
2.4.1 MAGE DEFENSOR 30
2.4.2 MAGE MK3 31

3 METODOLOGIA 33
3.1 Classificação da Pesquisa 33
3.1.1 Classificação Quanto aos Fins 33
3.1.2 Classificação Quanto aos Meios 33
3.2 Limitações do Método 33
3.3 Coleta e Tratamento dos Dados 33

4 DESCRIÇÃO E ANÁLISE DOS RESULTADOS 35

5 CONCLUSÃO 36
5.1 Considerações Finais 37
5.2 Sugestões para futuros trabalhos 37

REFERÊNCIAS 38

1. INTRODUÇÃO

O mundo contemporâneo ascende de maneira acelerada devido à constante evolução tecnológica. Nesse contexto, o papel de um Comandante é fundamental para o sucesso de uma operação militar. A atuação de um líder diante dos seus subordinados é empregada através do que é chamado de Comando e Controle (C^2). O C^2 possui diversos componentes, dentre os quais se encontra a comunicação e o tratamento das informações recebidas, visto que durante as operações é necessário empregar ações operacionais e estratégias de curtas e longas distâncias, onde, inclusive, emprega-se sistemas baseados em satélites, pois o principal requisito da comunicação é justamente a seguridade da mesma.

A aplicabilidade do C^2 tem aumentado de forma exponencial nos últimos anos, sendo muito referenciada por autores devido a sua grande relevância nas guerras modernas. Com apoio da Guerra Eletrônica (GE), o emprego da tecnologia da informação na guerra moderna faz com que a evolução das operações de guerra sobrevenha de forma a facilitar o trabalho do comando, no sentido de obter informações do campo de batalha. Entretanto, o uso das mesmas ferramentas da tecnologia da informação favorece exponencialmente o aumento de ameaças durante as operações de guerra.

1.1 Apresentação do Problema

O C^2 detém uma função crucial diante de uma operação militar, visto que a liderança favorecerá a ação de toda a operação. Entretanto, para que o C^2 possa contribuir de forma eficiente, precisa- se ter as informações necessárias para que a tomada de decisão possa ter um seguimento positivo. A GE e as suas medidas, como as MAGE, as MAE e as MPE, tendem a laborar em prol da obtenção das informações, a neutralização do inimigo e a proteção, respectivamente. O processo de obtenção das informações pode ser realizado de diversas formas, como, por exemplo, o uso de veículos aéreos não tripulados, radar ou sensores, porém, tais ações decorrem através do uso de espectro eletromagnético. O C^2 emprega a comunicação através de satélite, equipamento que emprega o espectro eletromagnético, sendo vulnerável às ações da GE.

1.2 Justificativa e Relevância

O estudo justifica-se através do fortalecimento do conhecimento que cerca a GE e o C^2, visto que a junção das duas ações permite o conhecimento sobre as ameaças, os sistemas de comunicação, posicionamento e todas as informações necessárias que podem ser consolidadas em uma operação. Tendo ciência da importância da filtragem e da distribuição de dados entre os níveis de Comando, pois o tratamento inadequado desses dados interfere na eficácia da estrutura do C², dificultando a tomada de decisão.

1.3 Objetivos

O propósito deste tópico é apresentar os objetivos que tendem a ser alcançados na elaboração deste trabalho, envolvendo um núcleo geral e específico, de forma a constituir a temática abordada.

1.3.1 Objetivo Geral

O objetivo Geral deste trabalho consiste na análise e na conceituação das vertentes que envolvem a GE e o C². .

1.3.2 Objetivos Específicos

Os seguintes objetivos específicos serão contextualizados:

a) Conceituar a Guerra Eletrônica: com o intuito de posicionar tais conceitos dentro da temática e abordar as medidas vertentes aplicadas na GE, como as Medidas de Ataque Eletrônico, Medidas de Proteção Eletrônica e Medidas de Apoio à Guerra Eletrônica;
b) Contextualizar as vertentes que se aplicam ao Comando e Controle;
c) Conceituar brevemente a Guerra de Comando e Controle;
d) Correlacionar a GE e sua aplicabilidade para o Comando e Controle, apresentando inclusive, as vulnerabilidades que decorrem dessa junção; e
e) Descrever os equipamentos que apoiam a tomada de decisão.

2. REVISÃO BIBLIOGRÁFICA

Neste capítulo serão apresentados conceitos relacionados ao tema, a fim de facilitar o entendimento da correlação entre a GE e o C², pois são fatores que influenciam diretamente no poder decisório em uma operação de guerra.

2.1 Guerra Eletrônica

A ligação entre guerra e tecnologia é demasiadamente intensa, fato este que demonstra o quanto a inovação tecnológica influencia no comportamento e direcionamento das guerras. Essa evolução constante parte diretamente da curiosidade e da criatividade humana diante do desenvolvimento de novas técnicas e metodologias que visam a resolução rápida ou eficiente das intercorrências. Cada processo inovador que ocorre ao longo dos anos, tende a favorecer o surgimento de conflitos, novos tipos de equipamentos e armamentos, assim como as estratégias e táticas de uso diante do contexto militar (BELLINTANI *et al*., 2014).

Figura 2.1: Interações eletromagnéticas.

Fonte: BRASIL, 2013.

A GE é utilizada no meio tecnológico há muitos anos, e sua história remonta à Segunda Guerra Mundial (IIGM). Durante a IIGM, o espectro eletromagnético (EEM) foi largamente empregado, consequentemente, a partir deste uso, a GE foi intitulada como "Guerra dos Feixes" neste período. Desse modo, a função inicial da GE era concentrada em mitigar o

impacto do radar de navegação utilizado para bombardear aeronaves, e mais tarde, passou a ser empregada não somente de forma aérea, mas terrestre e marítima em face das missões e diversas aplicações que decorrem do seu emprego (CESAR, 2013).

Portanto, a GE está relacionada aos resultados do processo de desenvolvimento de armamentos, táticas, equipamentos e tecnologia de comunicação ocorridos ao longo dos anos. No entanto, conforme mencionado anteriormente, este termo se aplica a todas as operações militares que usam emissões eletromagnéticas ou eletro-ópticas para evitar ações ou ataques inimigos.

Brasil (2014a) informa que a GE condiz com um agrupamento de ações que tendem a explorar as emissões eletromagnéticas (EEM) do oponente, com a finalidade de conhecer a sua ordem de batalha e a capacidade, para que as medidas sejam adequadas à situação, permitindo que sejam empregadas a redução ou prevenção dos sistemas utilizados de forma eficiente.

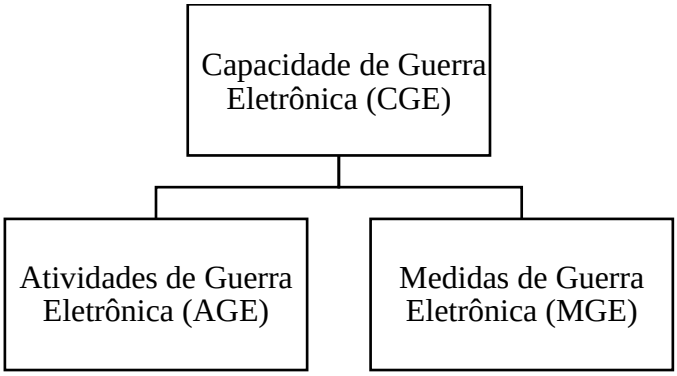
> O campo de batalha da guerra eletrônica é o aspecto eletromagnético. Como a matéria e a gravidade, a radiação eletromagnética é um dos componentes fundamentais do universo. Abrange uma larga faixa de frequências: desde as mais baixas, empregadas em enlaces de longo alcance, passando pelas faixas utilizadas em radiodifusão e nas transmissões de televisão, radares e ainda pela radiação infravermelha, incluindo o espectro óptico familiar da luz visível, de vermelho à violeta, até as mais altas, das radiações ultravioleta, raios X e gama (RICHARDSON, 1991, p. 24).

Visto isso, para favorecer o compreendimento sobre as ações da GE, abaixo serão apresentadas suas ações, sendo elas aplicadas através da conceituação da Capacidade de Guerra Eletrônica (CGE), das Atividades de Guerra Eletrônica (AGE) e das Medidas de Guerra Eletrônica (MGE).

2.1.1 Capacidade de Guerra Eletrônica

A CGE consiste em um somatório de recursos e procedimentos utilizados de forma eficiente nas operações em que a GE é empregada, favorecendo a aplicação proveitosa das estratégias logísticas e táticas (Fig. 2.2).

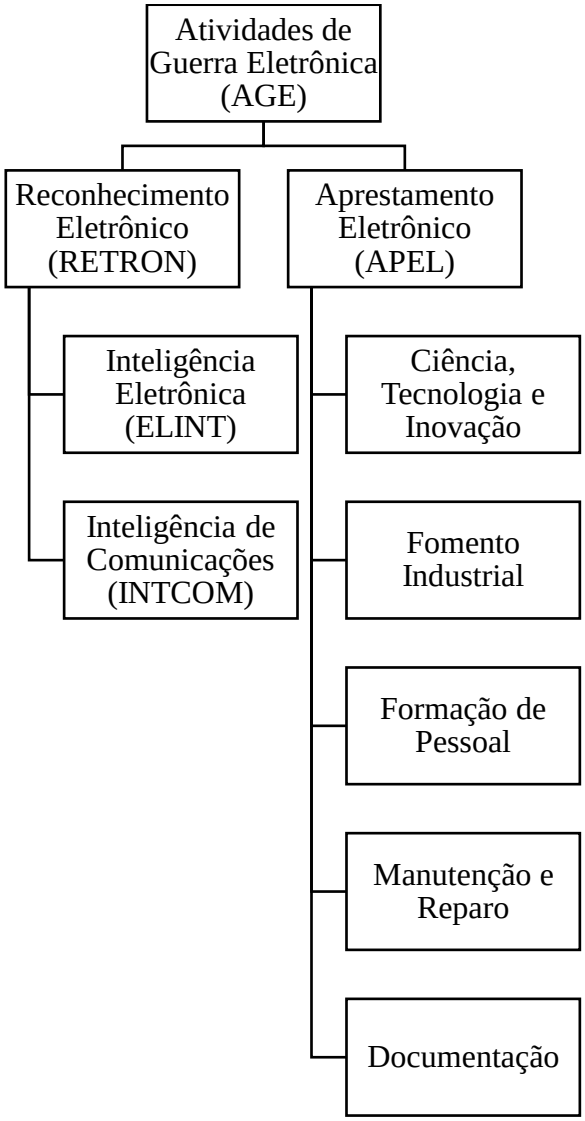
Figura 2.2: Divisão da Capacidade de Guerra Eletrônica (CGE).



Fonte: Elaborada pelo autor.

As Atividades de Guerra Eletrônica (AGE) decorrem do uso de estratégias de apoio durante as missões de guerra, portanto, estão relacionadas com artifícios logísticos, estratégicos e táticos que tendem a fundamentar as capacidades da GE diante das operações navais. Para favorecer a ação, dentro das AGE encontram-se o Reconhecimento Eletrônico (RETRON), que é empregado com o propósito estratégico ou apoio ao planejamento de uma operação, visando à obtenção e ao processo sistemático de informações sobre a CGE do inimigo; Inteligência Eletrônica (ELINT), que visa a obtenção de parâmetros técnicos através da interceptação de sinais que utilizem EEM e utiliza equipamentos para a produção de informações (sensoriamento); Inteligência de Comunicações (INTCOM), que visa a obtenção de parâmetros técnicos e outros a partir da interceptação de sinais de sistemas de comunicação e utiliza equipamentos para o trânsito de informações; e o Aprestamento Eletrônico (APEL), que reúne medidas de prontificação ou preparo compreendendo atividades de pesquisa, de desenvolvimento, de logística e de capacitação de recursos humanos (BRASIL, 2019) (Fig.2.3).

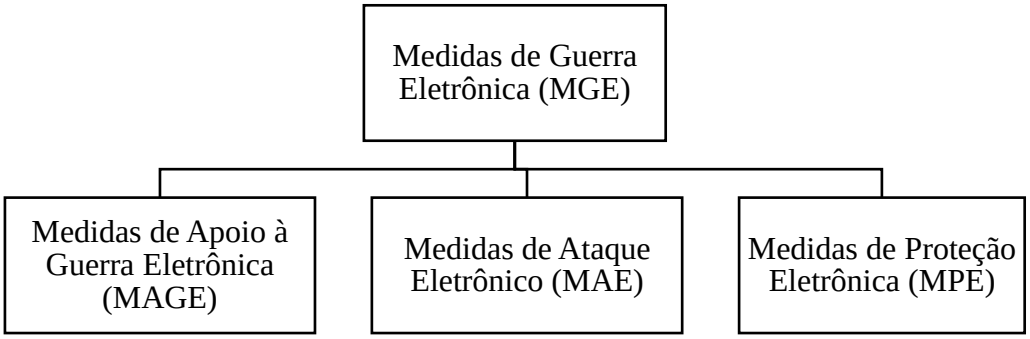
Figura 2.3: Ações básicas da AGE.



Fonte: Elaborada pelo autor.

As MGE ressaltam as ações da CGE atuando diretamente nas operações de guerra. Por essa razão, as MGE possuem subdivisões para ampliar as suas ações, sendo elas divididas em Medidas de Apoio à Guerra Eletrônica (MAGE), Medidas de Ataque Eletrônico (MAE) e Medidas de Proteção Eletrônica (MPE) (Fig. 2.4).

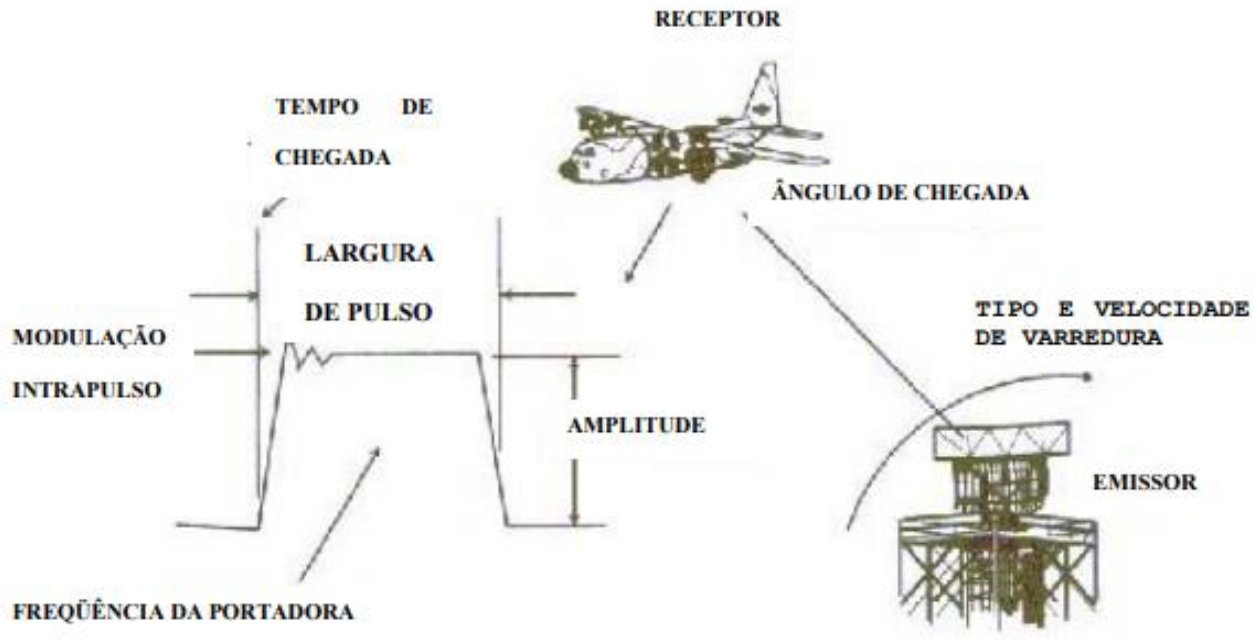
Figura 2.4: Organograma da MGE.



Fonte: Elaborada pelo autor.

As MAGE são projetadas com o intuito de obter informações para o sistema de C² do navio, a fim de apoiar a tomada de decisão com base nas características de ataque conduzidas pelo equipamento. Portanto, o dispositivo MAGE intercepta a transmissão de acordo com os parâmetros (ângulo de chegada, tempo de chegada, largura de pulso, frequência, entre outros) de cada radar interceptado, armazena o sinal e realiza a medição. Distância e amplitude, pois a prioridade é a identificação de ameaças e a associação de armas e radares inimigos (Fig. 2.5) (DRISCOLL *et al*., 1999).

Figura 2.5: Parâmetros medidos pelo sistema MAGE.

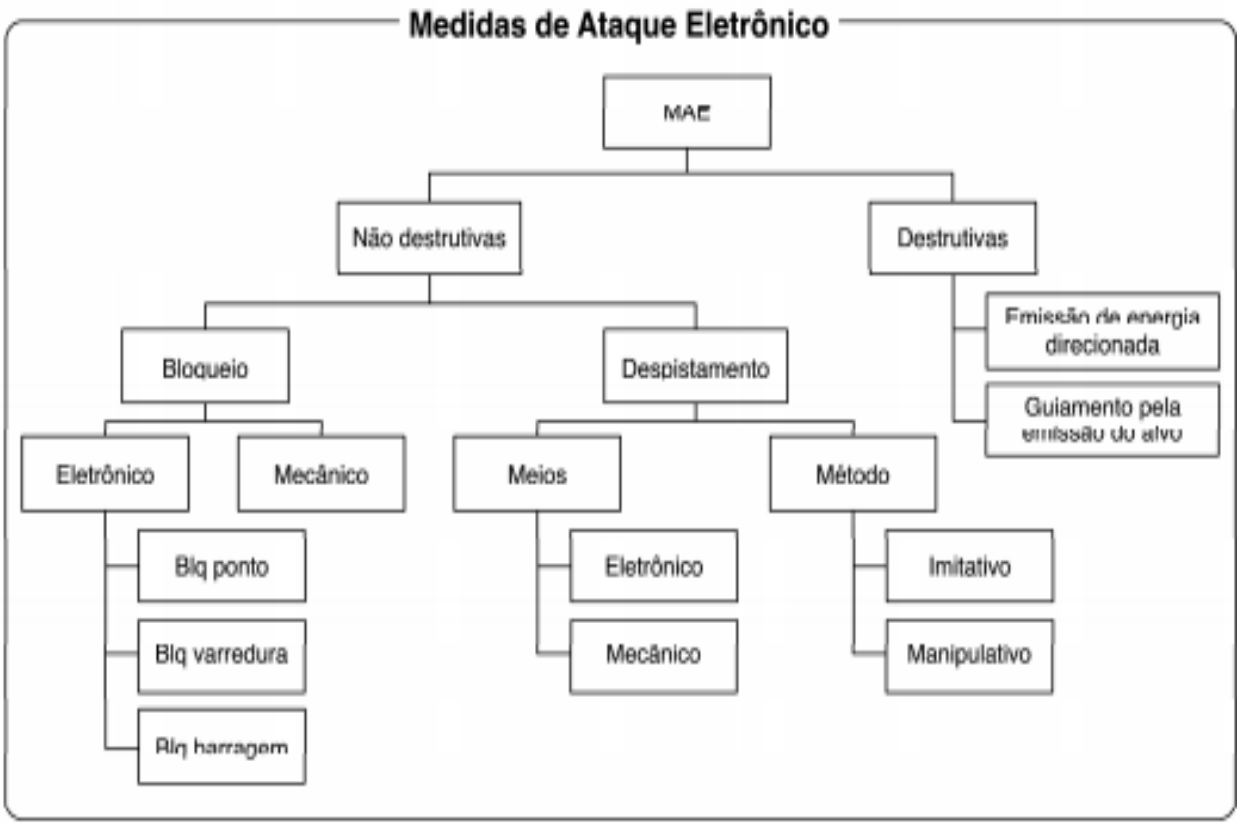


Fonte: BRASIL, 2013.

As MAE consistem em um agrupamento de ações que visam o impedimento, a neutralização ou a atenuação do EEM utilizado pelo inimigo, diminuindo a sua capacidade de combate através dos armamentos empregados durante a operação. Para isso, as MAE (Fig. 2.6) favorecem o processo de ataque, corroborando com a proteção, despistamento e comunicação

da operação através das suas subdivisões denominadas como MAE Destrutiva (Hard Kill) e MAE Não-Destrutiva (Soft Kill) (BRASIL, 2014a).

Figura 2.6: Medidas de Ataque Eletrônico.



Fonte: BRASIL, 2019.

Como o âmbito marítimo está sujeito a vários tipos de ataques eletrônicos, é necessário tomar medidas para garantir a utilização do espectro eletromagnético, portanto, as MPE são utilizadas, visto que sua função é garantir que os equipamentos utilizem EEM, sem intercorrências, protegendo o pessoal, os meios, as instalações e os equipamentos. As MPE subdividem-se em ações ANTI-MAGE e ANTI-MAE.

As ANTI-MAGE funcionam através de criptografia e codificação, empregada para proteger a comunicação durante as operações, empregando variação da frequência de sinal para enfraquecer o tráfego, antenas direcionais e *deinterleaving* por meio de sequência direta[1] (POISEL, 2011).

As ANTI-MAE atuam através do salto de frequência[2], sendo este empregado com

[1] Técnica que visa geração múltiplas cópias dos sinais que são espalhadas no espectro eletromagnético, reduzindo a potência de pico do sinal transmitido (POISEL, 2011, p. 7).

[2] Técnica de sistema na qual o equipamento altera a sua frequência de transmissão rápida (às vezes em milésimos de segundo), sistematicamente e seguindo uma sequência pseudoaleatória, fazendo com que um bloqueador tenha um tempo de atraso para identificar a nova frequência a ser atacada ou tenha que dividir sua potência de bloqueio em uma grande faixa do espectro (POISEL, 2011, p. 8-9).

a finalidade de atenuar a eficácia do ataque eletrônico empregado pelo inimigo. Desse modo, nestas ações também se consideram a utilização da criptografia, para que o despistamento imitativo e a autenticação da seguridade possam ser dificultados, corroborando para que a comunicação recebida seja diretamente da comunicação de origem durante as operações. Outra possibilidade de emprego nesta situação, consiste no uso de antenas direcionais, visto que elas dificultam uma operação de ataque eletrônico, o que fará com que o inimigo aumente a sua potência para que o ataque seja mais eficiente (POISEL, 2011).

2.2 Comando e Controle

2.2.1 Conceituação de Comando e Controle

A conceituação de C^2 pode ser entendida através de diversos significados e abordagens, desde o emprego de sistemas computacionais modernos, à guerra. Contudo, compreende-se que o C^2 visa a seguridade das informações dentro de uma operação, atenuando desta forma os fenômenos denominados como fricção da guerra (decorre dos resultados inesperados em função das intenções do comandante ao que se diz respeito as ações) e névoa (decorre através das incertezas sobre o que está ocorrendo).

De acordo com Acácio (2018), o C^2, apesar de separados, tem suas conexões, enquanto um tem o objetivo de tomar decisão exercendo a sua liderança, o outro tem a finalidade de empreender ações por meio da avaliação e correção das atividades, de forma a não permitir que se perca o propósito estabelecido. Com isso, o Comando é o responsável por enviar as Forças para determinada missão e o Controle trabalha com o monitoramento e a análise das ações empreendidas.

Para a Marinha do Brasil:

> C^2 é uma atividade fundamental para o êxito das operações militares em todos os escalões de comando. Como atividade especializada, sua execução se baseará em uma concepção sistêmica, com métodos, procedimentos, características e vocabulário que lhe são peculiares. Vincula e permeia todas as atividades operacionais e de apoio, sincronizando-as e permitindo ao comandante adquirir e manter o indispensável nível de consciência situacional para a tomada de decisões adequadas às circunstâncias do ambiente operacional, para a expedição de ordens e para o controle de sua execução (BRASIL, 2015a, p. 12).

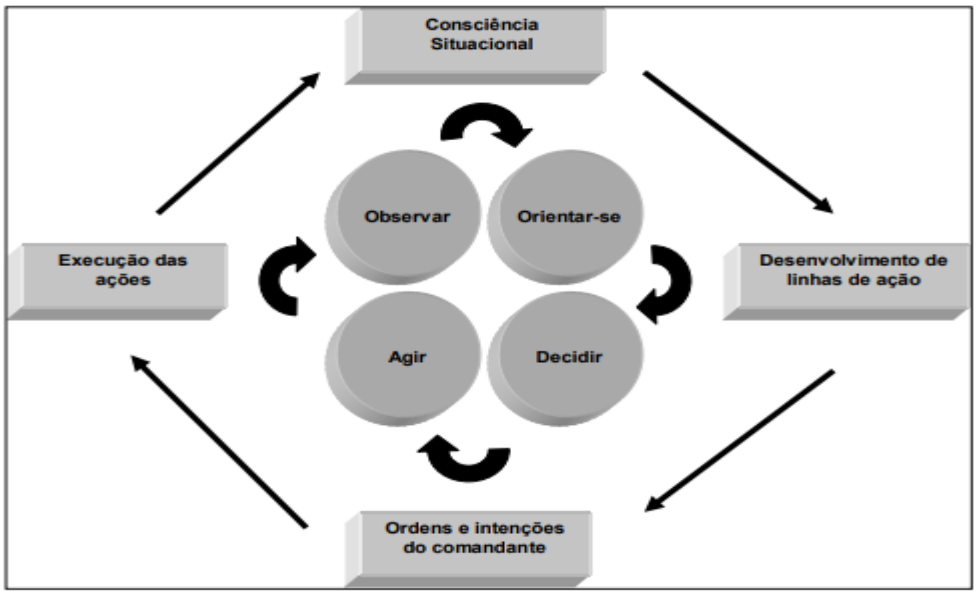
Coakley (1992) torna a conceituação da C^2 mais abrangente, defendendo que ela decorre da comunicação dos comandantes com seus subordinados e superiores; do

conhecimento sobre as missões; do acesso às informações sobre os inimigos, sobre o planejamento, sobre a liderança e de como uma operação decorre através do planejamento; e do trabalho liderado pelo C^2. Apesar da definição parecer que todo o processo decorre individualmente e por fase, eles são interligados e empreendidos através do comandante e toda a estrutura que envolve o C^2, o que torna o processo interativo e dinâmico.

O processo decorrente das ações de C^2 pode ser compreendido pela efetivação do Ciclo de Boyd ou OODA (Fig. 2.7). O nome deste ciclo é resultado de uma junção das palavras, Observar, Orientar, Dirigir e Agir. O Observar decorre da obtenção de todas as informações necessárias para que as operações sejam realizadas adequadamente. Orientar relaciona-se com a compilação das informações obtidas. Decidir consiste no processo de tomada de decisão. Agir consiste na ação resultante da decisão (BORGES, 2007).

A vertente conceitual do Reconhecimento Eletrônico (RETRON) considera o OODA como ciclo de decisão ou de C^2. As etapas desse ciclo são realizadas por meio de comunicações, quanto antes interceptar essa comunicação melhor será para a identificar as intenções dos inimigos, pois só se toma conhecimento dessas ações, depois que as mesmas são iniciadas e podem ser observadas por nossas redes de sensores. Com isso é possível antecipar o início do ciclo e obter vantagens sobre o oponente.

Figura 2.7: Ciclo de OODA.



Fonte: BRASIL, 2019.

Desse modo, entende-se que o ciclo tende a se repetir de forma contínua, tratando e buscando informações que podem interessar ao comandante da operação, no processo do cumprimento desta, assim como, realizar uma análise das ações e a transmissão das determinações.

> Ao confrontar-se com um cenário dinâmico e abrangente, o comandante percebe que o aprimoramento do processo decisório é essencial para garantir a vantagem competitiva. Nesse contexto, destaca-se a atividade de comando e controle (C^2), no qual a estrutura correspondente, o sistema e o decisor são os componentes básicos (VIVEIROS, 2007, p.8).

As atividades executadas de C^2 são desenvolvidas em um Centro de Operações, denominado como Centro de Comando e Controle, configurado para permitir a ligação entre o comando e estrutura militar, a fim de que seja integrado o conhecimento das ações de forma imediata para que, quando necessário, correções e ajustes possam ser empregados em tempo real. Por essa razão, entende-se que a estrutura do C^2, de forma conjunta, é responsável pelo funcionamento satisfatório da cadeia de comando, o que permite que as informações possam chegar ao destino rapidamente, favorecendo a tomada de decisão por parte do comandante (BRASIL, 2015a).

Contudo, compreende-se que equipamentos e seres humanos estão sujeitos a serem falhos, e por mais que a tecnologia seja sofisticada, a velocidade de evolução das guerras pode corroborar para que o comandante tenha a falsa impressão de que as informações recebidas durante as operações são precisas (VIVEIROS, 2007). Devido a isso, para que as tecnologias possam favorecer positivamente as operações, as pessoas que operam os equipamentos devem ser devidamente capacitadas e qualificadas para explorá-los ao máximo (GARCIA *et al*., 2005).

Entretanto, de acordo com Coakley (1992), a flexibilidade humana e o senso comum superam a lógica e a razão, visto que a mente humana possui a capacidade de explorar amplas possibilidades que são desconsideradas por equipamentos, apesar das máquinas possuírem maior capacidade de armazenamento de dados e de raciocino lógico. Viveiros (2007) complementa a pontuação do autor anterior, informando que as máquinas e serem humanos possuem vulnerabilidades, bem como os fatores de força, que quando unificados corretamente, tendem a favorecer o emprego eficiente de todas as vertentes que englobam o C^2.

Desse modo, observa-se que a estrutura ideal da C^2 é aquela que permeia através da Tecnologia da Informação[3] (TI), para permitir que o comandante possa ter o conhecimento sobre as ações em andamento, sobre as informações necessárias e o tempo em que elas ocorrem, empregando um tráfego de informações e as ordens decorrentes das mesmas, de forma segura e confiável. Independente da definição empregada para o C^2, as suas atividades empregam ações complexas e inovações tecnológicas, assim como o preparo do pessoal envolvido nas

[3] Conjunto formado por pessoal técnico e qualificado, processos, serviços e recursos tecnológicos, incluindo equipamentos e programas que são utilizados na geração, no armazenamento, na veiculação, no processamento, na reprodução das informações (VIVEIROS, 2007, p.12).

operações, permite que diversas quantidades de informações sejam disponibilizadas para circularem em uma determinada rede, sendo acessadas e atualizadas, a fim de favorecer a decorrência de uma operação.

2.2.2 Sistema Naval de Comando e Controle

Corroborando com a definição anteriormente apresentada, pode-se afirmar que a estrutura de C^2 da Marinha do Brasil consiste em um agrupamento de equipamentos, instalações, doutrinas, comunicações, procedimentos e pessoas que são primordiais para que o Comandante possa dirigir e planejar as ações navais e a execução das missões (BRASIL, 2001). Esse agrupamento é diretamente inserido em uma rede organizacional denominada como Sistema Militar de Comando e Controle, sendo este dividido em: estratégico, tático operacional e político. O Comandante do Teatro de Operações Marítimas (COMTOM) é a autoridade de maior escalão do Sistema Naval de Comando de Controle ($SISNC^2$)[4] e possui o controle dos níveis táticos e operacionais, tratando-os através de estratégias, visto que o sistema de C^2 disposto ao $SISNC^2$ deve permitir e favorecer o fluxo de informações (BRASIL, 2015b).

Desse modo, com o intuito de favorecer o fluxo de informações foi empregado um software mais sofisticado, com capacidade de apresentar os cenários de guerra graficamente e o posicionamento das plataformas desconhecidas, inimigas e amigas.

A criptografia desenvolvida pelo Centro de Análises de Sistemas Navais (CASNAV) é empregada juntamente com o Software do $SISNC^2$, com o intuito de favorecer a comunicação segura entre os centros de rede, proporcionando que as informações cheguem a todos os níveis da operação através da rede estabelecida. Todo esse processo ocorre dentro da Rede de Comunicação Integrada da Marinha (RECIM)[5] e do Sistema de Comunicações Militares por Satélite (SISCOMIS). Visto isso, ainda pode ser estabelecido um enlace com restrições de velocidade para que a seguridade da comunicação possa ser empregada de forma eficiente, sendo utilizado equipamentos comerciais por satélite e, na ausência deste meio, utiliza-se um conjunto modem-rádio de alta frequência (HF) devido a sua aplicabilidade em longas distâncias (FELIX, 2008).

---

[4] Na física, chama-se capilaridade à propriedade dos fluidos de subir ou descer em tubos muito finos. Em um sistema de Comando e Controle, o efeito de capilaridade visa manter um fluxo vertical de dados desde o mais alto escalão e as menores frações de uma força ou grupamento militar.

[5] A RECIM é a rede do serviço de comunicações das unidades de terra da MB, que interliga as estações terrestres fixas e navios atracados, por meio de linhas físicas ou enlaces de micro-ondas (FÉLIX, 2008).

2.2.3 Satélite de comunicação e a sua aplicabilidade no SISCOMIS

A comunicação é a aplicação mais importante diante do uso de satélites, visto que este funciona como uma estação repetidora do sinal recebido por uma estação terrestre e, por isso, o mesmo é empregado em diversos tipos de serviços de comunicação como telefonia, internet, tráfego de dados corporativos, comunicação militar, entre outros (MAINI *et al*., 2011).

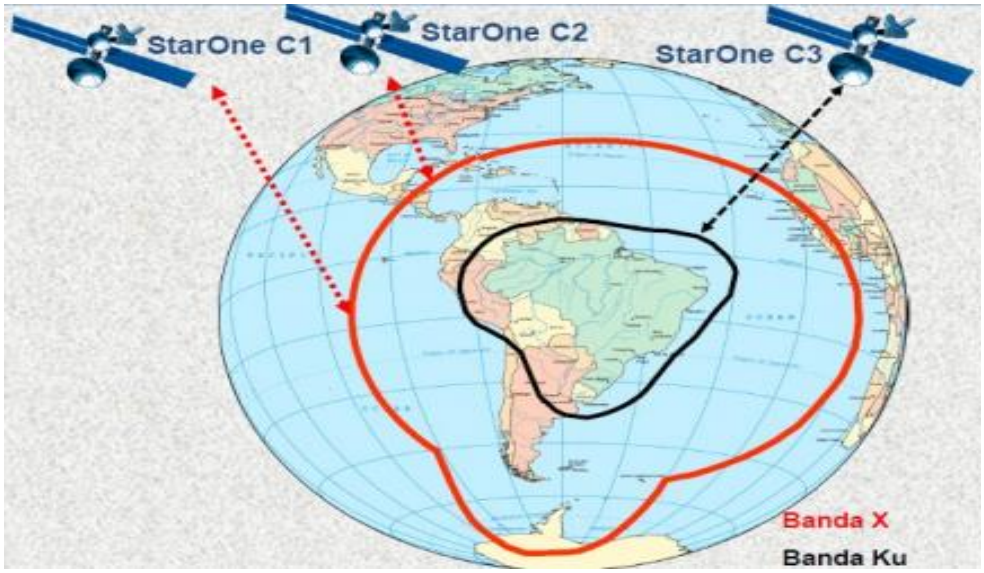
O SISCOMIS foi criado com o intuito de favorecer a interligação entre os centros de C² das Forças Armadas e o Estado-Maior de Defesa, proporcionando enlace com seguridade e confiança. Além disso, este sistema é composto por um agrupamento de estações fixas (Fig. 2.8), estabelecidas em estações móveis, centros urbanos, navios ou plataformas, para que seja possível acompanhar as tropas. Os satélites utilizados pelo SISCOMIS (Fig. 2.9) são do tipo geoestacionário, lançados a 36.000 km da superfície terrestre, com velocidade de característica orbital e tornando-se estacionário posteriormente (MAINI *et al*., 2011).

Um satélite de comunicação militar é empregado nas ações de C^2 visando a tramitação de informações de forma segura, interoperável, confiável, móvel e contínua, como por exemplo, videoconferências, telefonia, acesso a sistemas digitais operativos, tráfego de imagens e até mesmo telemedicina. Compreende-se dessa forma, que este meio de comunicação pode ser empregado de forma tática e conjunta para aumentar a rede de alcance em UHF. Essa correlação pode ser observada através da (Fig. 2.10).

Figura 2.8: Estação Fixa do SISCOMIS.

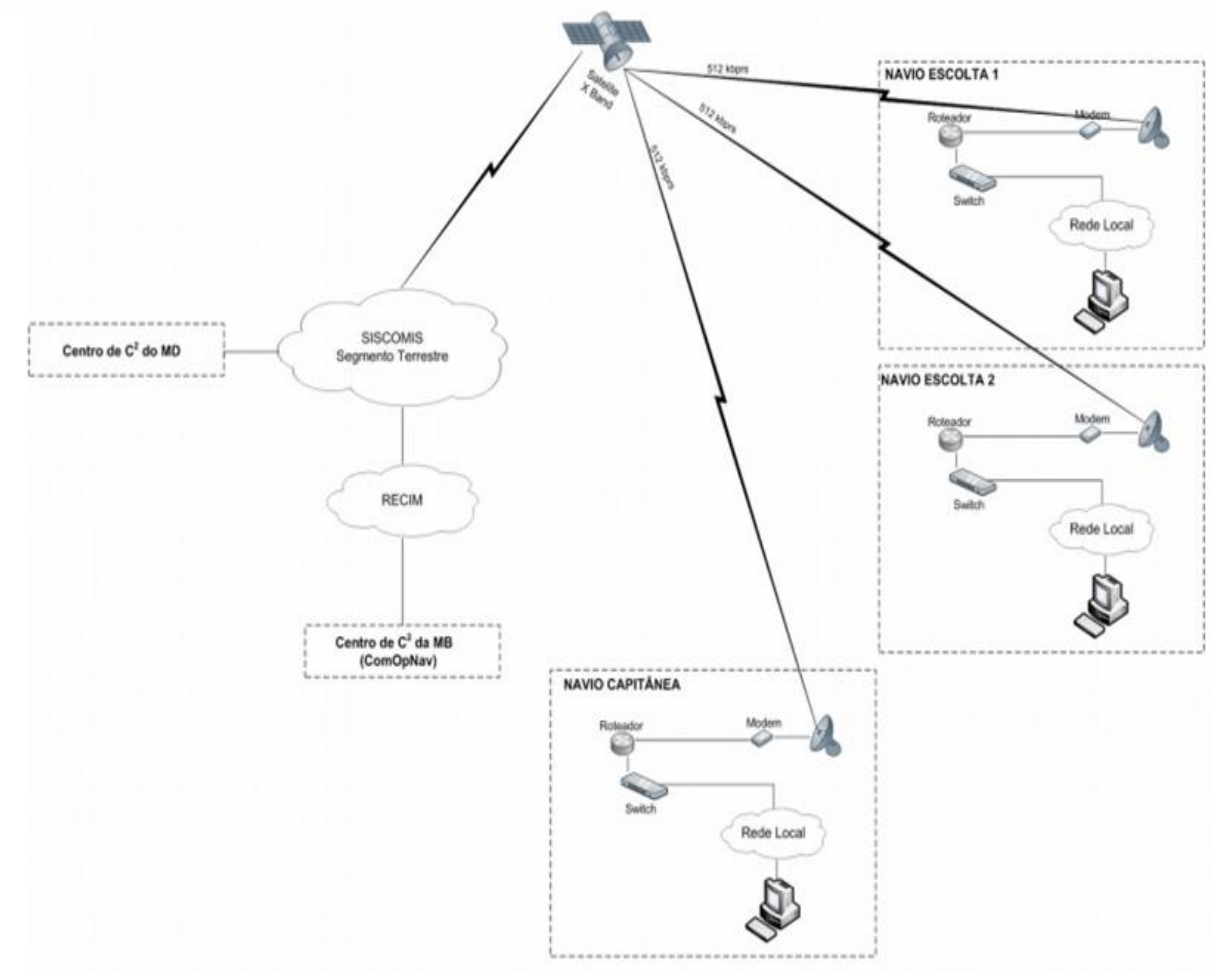
Fonte: SILVA, 2009.

Figura 2.9: Área de cobertura satelital do SISCOMIS.



Fonte: BRASIL, 2014a.

Figura 2.10: Recursos do SISCOMIS.



Fonte: VIVEIROS, 2007.

2.2.4 Importância da Informação

A informação sempre possuiu relevância para que o homem pudesse interpretar e perceber situações, onde a partir dela, gerar decisões que também seriam transmitidas por meio de informações. A importância da informação não é um fator novo, visto que pensadores como Sun Tzu e Clausewitz já citam sobre a sua importância e a força que ela possui, além de afirmar que quando conhecemos as nossas forças e não as do inimigo, ocorrerá uma derrota para cada vitória (TZU, 2006).

De acordo com Viveiros (2007), as informações diante do C² possuem grande importância, sendo esta inclusive capaz de paralisar a ação de guerra, pois esta é a matéria prima de maior valor diante do exercício da C^2. O Comandante, quando de posse de todas as informações vertentes às forças e inimigos, tende a combiná-las juntamente com o conhecimento e treinamento que possui, em prol de um processo decisório e de controle conforme a decorrência da operação de guerra.

2.2.5 A Guerra de Comando e Controle

A utilização de armamento pode neutralizar ou até destruir Centros de Comando, como mísseis e bombas. Contudo, avaliando o contexto de guerra, entende-se que o ataque direto não é a única forma, visto que as instalações são ambientes susceptíveis, como, por exemplo, ao corte de energia ou a um vírus empregado na rede de comunicação.

A Guerra de Comando e Controle pode ser definida como:

> O uso integrado de segurança das operações, despistamento, operações psicológicas, guerra eletrônica e destruição física, apoiadas pelas atividades de inteligência, para negar informações, influenciar, degradar ou destruir as capacidades de C² do oponente e protegendo as forças amigas contra tais ações. A Guerra de Comando e Controle é uma das formas da Guerra de Informação empregada em operações militares, sendo aplicável a todos os níveis do conflito (UNITED STATES, 2001, p. 80).

Além disso, é necessário que o C^2 empregue no decorrer das ações de guerra, uma operação de reconhecimento para comparar os poderes das forças amigas e inimigas. Nesta análise, segundo Brasil (2001), confronta-se as seguintes pontuações:

a) Condições em que o comando é empregado, em termos de transmissão de ordens, estrutura, características decisórias e estratégias;
b) Sistemas de sensores, computacionais, comunicação e de GE disponíveis na operação; e
c) Desempenho e eficiência dos sistemas diante do apoio decisório das ações.

Após a análise e conhecimento sobre os fundamentos da operação de Guerra, tornar a operação uma ação ofensiva será mais fácil, isto é, fazer com que o inimigo feche olhos e ouvidos através do emprego de criptografia no trâmite de informações, visto que, atenuando o fluxo interceptável, a tomada de decisão e o ciclo decisório do oponente serão prejudicados, favorecendo o trabalho das forças amigas. Desse modo, ao reconhecer a importância das ações da C^2, sendo esta aliada ao avanço da tecnologia e a contínua adaptação do homem, compreende-se como uma operação de guerra deve ser conduzida.

2.3 **Guerra Eletrônica x Comando e Controle**

No decorrer da revisão apresentada em tópicos anteriores, foi realizada uma conceituação breve de todos os conceitos vertentes à GE e do C^2 para favorecer o compreendimento e a correlação que as ações de ambos possuem quando empregados em operações de guerra.

A agilidade de trabalho do C^2 decorre dos meios de comunicação, por isso emprega-se que as informações decorrentes sejam confiáveis, seguras, rápidas, flexíveis e integrativas, partindo do ponto de que a estrutura de C^2 possa ser modificada ou até pensada em conformidade com a missão (BRASIL, 2014a).

Como citado anteriormente, a GE decorre do emprego de ações que visam a explorar as emissões do inimigo em toda a faixa do EEM, com a finalidade de conhecer a sua ordem de batalha, suas intenções e capacidades, e, também, utilizar medidas adequadas para negar o uso efetivo dos seus sistemas, enquanto se protege e utiliza, com eficácia, os sistemas próprios (BRASIL, 2019).

Desse modo, entende-se que a GE e as suas ações contribuem em prol da execução da operação, com a obtenção das informações sobre o inimigo (localização, distância, amplitude, largura de pulso, entre outros), as MAGE, as MAE e as MPE, a fim de proteger a comunicação da tripulação e do Comandante durante a operação de guerra. O C^2 utiliza as informações recebidas para que as operações possam ser direcionadas adequadamente.

Entretanto, durante uma operação de guerra, a GE visa a interferência do seu alvo principal, o C² do inimigo (no ataque) ou amigo (proteção).

Visto isso, ambas as ações fornecem informações sobre forças inimigas e amigas, e, por isso, abaixo será contextualizado a correlação entre as ações de GE com o foco em MAGE, MAE e MPE, e a Inteligência de Sinal (INTSAL) empregada pelo C^2 nas operações.

2.3.1 MAGE e Inteligência de Sinal

As MAGE e a INTSAL visam a exploração quanto ao uso de EEM pelo oponente durante uma operação de Guerra. Contudo, as MAGE buscam as informações com o intuito de favorecer a operação de guerra de forma imediata, enquanto o INTSAL visa a coleta de informações sobre sistemas de comunicações e sensores eletrônicos para permitir o desenvolvimento do trabalho do C^2, e auxiliar as CGE para que o seja eficiente durante as operações. Ambos estão correlacionados de forma operacional por meio da troca de dados e informações (BRASIL, 2019).

A INTSAL e as MAGE vão iniciar o processo de análise através da busca EEM, uma vez identificado, o sinal de interesse para a operação será monitorado e as informações obtidas serão armazenadas. Conforme Vieira (2008), esta análise de sinal emprega cinco vertentes, sendo elas:

a) Mensagem - a análise da mensagem visa a produção de informações, sendo elas decodificadas após a recepção do sinal;
b) Tráfego - a análise do tráfego decorre das informações obtidas através das mensagens, sendo possível determinar a aplicabilidade da rede diante da operação (tática ou estratégica);
c) Localização - a análise da localização visa conhecer o posicionamento do inimigo;
d) Técnica - a análise da técnica visa o conhecimento dos parâmetros de sinal, como a codificação, modulação e frequência, a fim de favorecer o conhecimento sobre o tipo de inimigo que se encontra no campo de guerra e a base de equipamentos empregados; e
e) Fase Final - a análise final é a que realiza a integração de todas as informações obtidas.

Desse modo, comparando o ciclo de C², a análise conceitual de MAGE e INTSAL, observa-se que como um sensor, ambos contribuem para a observação e a obtenção de informações, parte de extrema importância diante do trabalho do C^2. Sendo assim, ao empregar o monitoramento das comunicações através dos sinais ou emissões EEM, é possível empregar

medidas antes mesmo do oponente iniciar o ataque. As ações da GE contribuem para que não seja mais necessário esperar por uma decisão e nem esperar que o sensor detecte (por exemplo, a transferência de tropas) a ação, pois as ordens podem ser interceptadas e até mesmo o comandante pode ser consultado para perguntar por quanto tempo as tropas estão preparadas para se mover.

Com isso, o processo de planejamento deve ser totalmente analisado com antecedência para subsidiar o processo de tomada de decisão do Comandante. Este é um dos métodos eficazes observados, o ser capaz de "entrar" no processo de tomada de decisão do adversário e prever suas ações naturalmente através das inovações tecnológicas. Entretanto, os riscos estratégicos devem sempre ser analisados com cuidado e esses dados não devem limitar a análise das possibilidades do inimigo por parte do C^2.

2.3.2 MAE

As MAE subdividem-se em MAE Destrutiva e MAE Não-Destrutiva, contudo, o tópico em questão será direcionado somente a Não Destrutiva. As MAE Não-Destrutiva dividem-se em supressão eletromagnética (bloqueio), despistamento e energia direcionada, como apresentando anteriormente. O objetivo do bloqueio empregado pelas MAE é interromper a comunicação em um determinado momento, dessa forma a fim de viabilizar o uso de sistemas ou acarretar retardos na comunicação inimiga. Já o despistamento visa a indução de erro ao sistema inimigo através de informações falsas (POISEL, 2011).

Com base no que foi descrito, fica claro que as MAE visam alcançar a comunicação de duas maneiras diferentes. Em primeiro lugar, espera-se que as comunicações sejam interrompidas, embora temporariamente e, conforme introduzido no conceito de C^2, essa medida causará o atraso no C^2 e na condução do ciclo de Boyd do inimigo, influenciando nos princípios de confiabilidade, continuidade e velocidade. Contudo, por outro lado, o despistamento imitativo pode causar confusão, prejudicando os aspectos cognitivos do processo de tomada de decisão em todos os níveis da operação, prejudicando, assim, os princípios de segurança. Sua função é expandir a névoa da guerra, o que acarretará efeitos secundários, como ser descoberto, afetando a credibilidade de todos os julgamentos feitos até aquele momento da operação. Isso também atrasará o ciclo C^2 para que os fatos conhecidos possam ser reavaliados.

2.3.3 MPE

Segundo Brasil (2019), as MPE são o conjunto de ações defensivas que buscam assegurar o uso eficiente e eficaz do EEM pelas forças amigas, não obstante o eventual emprego das MAGE e MAE pelo oponente ou, ainda, pelas próprias forças. Suas ações têm a finalidade de salvaguardar pessoal e material dos efeitos decorrentes do uso do EEM que degradem, destruam ou inviabilizem a capacidade de combate dos aliados. São representadas pelas ANTI-MAE e ANTI-MAGE.

As ANTI-MAGE constituem um conjunto de ações que visam evitar que o inimigo utilize os sistemas de INTCOM e/ou de ELINT das forças como fontes de informações, negando-lhe o sucesso nas ações MAGE (Busca de Interceptação, Monitoração, Localização Eletrônica, Registro e Análise de GE) e, consequentemente, impedindo a ação de dados. São de vital importância para a segurança de toda a tropa, devendo ser realizadas permanentemente. As ANTI-MAE constituem um conjunto de ações a serem tomadas no instante em que o operador de um equipamento da INTCOM ou da ELINT identifica que está sendo alvo de ações de MAE. (BRASIL, 2014b).

Desse modo, ao analisar as informações acima, compreende-se que as MPE, para serem empregadas, exigem a existência de ameaças e só ocorrem as ameaças, justamente pelo emprego das MAGE/INTSAL e das MAE. Correlaciona-se esse processo com o emprego da criptografia na comunicação empregada pelo C^2 para prioritariamente proteger as informações da operação e a interceptação destas, mas, secundariamente, dificultará o emprego das MAE, o que torna a ação sem sentido, pois, caso ocorra a instalação da criptografia, as ameaças não serão corretamente identificadas pelo sistema utilizado pelas forças amigas.

2.3.4 Breves considerações sobre a GE como auxílio para o C^2

As ações da GE, ao que se diz respeito à comunicação empregada durante uma operação de Guerra, tende a favorecer as ações e a tomada de decisão do C^2, uma vez que, para iniciar uma ação contra um inimigo é necessário ter todas as informações sobre a operação, antes de iniciá-la. Além disso, o emprego das ações favorece também o conhecimento do processo cognitivo e as possibilidades de ação do inimigo, o que fará com que o C^2 amigo possa antecipar as ações adversárias.

Uma das ações pertencentes às MAE é a interrupção do sinal de comunicação, prejudicando a cognição e o processo decisório e favorecendo a névoa de guerra, interrompendo

a eficácia da operação, mesmo que temporariamente, e ocasionando atrasos no Ciclo de ação do C², assim como o Ciclo de Boyd ou OODA.

Nota-se que há a presença de vulnerabilidade da comunicação através de satélites quando são empregadas as ações da GE nas operações, visto que a mesma atua através das emissões eletromagnéticas, sendo está a base da comunicação satelital.

Abaixo, encontra-se uma tabela correlacionando as ações de C^2 com os componentes da GE, sendo está uma breve análise.

Tabela 2.1: Correlação entre GE e C^2.

AMEAÇA	**PRINCIPIOS DO C^2**	**GE**
Monitoramento	Segurança	MAGE/INTSAL
Interrupção do sinal	Confiabilidade, Continuidade e Rapidez	MAE
Simulação de Comunicação Falsa	Segurança	MAE

Fonte: Elaborada pelo autor.

2.4 Equipamentos empregados no auxílio ao C²

2.4.1 MAGE DEFENSOR

O MAGE DEFENSOR foi desenvolvimento pelo Instituto de Pesquisa da Marinha (IPQM) na década de 90, juntamente com a empresa ELEBRA e OMNISYS. O DEFENSOR baseia-se no Sistema Operacional Linux e foi instalado na Corveta Barroso e no Navio Escola Brasil. As principais características deste MAGE serão apresentadas abaixo:

Tabela 2.2**:** Aspectos do DEFENSOR.

ASPECTOS	**DESCRIÇÃO**
Faixa de frequência	É capaz de detectar um sinal eletromagnético somente acima de 2GHZ.
Biblioteca de emissão	Devido a integração com o sistema fênix, as classificações das ameaças são realizadas de forma automática, com apresentação em tela e sugestão de resposta contra ameaça utilizando as técnicas de MAE e o empregado do SLDM em conformidade com o nível de ameaça detectado.

ELINT	Possui a ELINT, sendo uma funcionalidade específica, além disso o DEFENSOR atua de forma estratégica, realiza gravações, armazenamento de áudio ambiente (são gravados em forma bruta e utiliza um sistema processador chamado SW disponível em CGEM). O sinal gravado através do ELINT é mais rico em informações, pois o mesmo realiza a gravação antes mesmo do processamento e a análise dos sinais são realizados posteriormente; Possibilidade do incremento do banco de dados da Marinha do Brasil, proporcionando funções estratégicas de RETRON e de APEL.
Detecção de radares com diversidade de frequência (LPI).	Pode atender a detecção de diversidade de frequência (LPI) e consiste na principal diferença funcional em conexão com B1BW quando identifica o radar LPI como um único ruído;

Fonte: Elaborada pelo autor. Baseado em Alves (2020).

Além disso, outros aspectos devem ser mencionados, como apresentado por Alves (2020):

a) A distância entre o DEFENSOR e a Unidade de Processamento (UP) é de 25 metros, permitindo um compartilhamento mais abrigado próximo a linha de água;
b) Por ser um produto nacional, há diversas vantagens de acordo quanto a sua manutenção. Entre essas vantagens, eles enfatizam: menores custos, reduzindo os custos de obtenção de peças de reserva; Custos mais baixos de reparação; Maior disponibilidade de trabalho para reparos; Maior confiabilidade em reparos;
c) Ele tem integração com o sistema Fênix, permitindo os fins de classificação automatizados detectados pela MAGE com as constantes da biblioteca de fênix. Essas são todas as características do objetivo apresentadas na tela, bem como no nível deste objetivo; e
d) Permite a análise de todo o agrupamento de emissão eletromagnética recebidas de forma precisa.

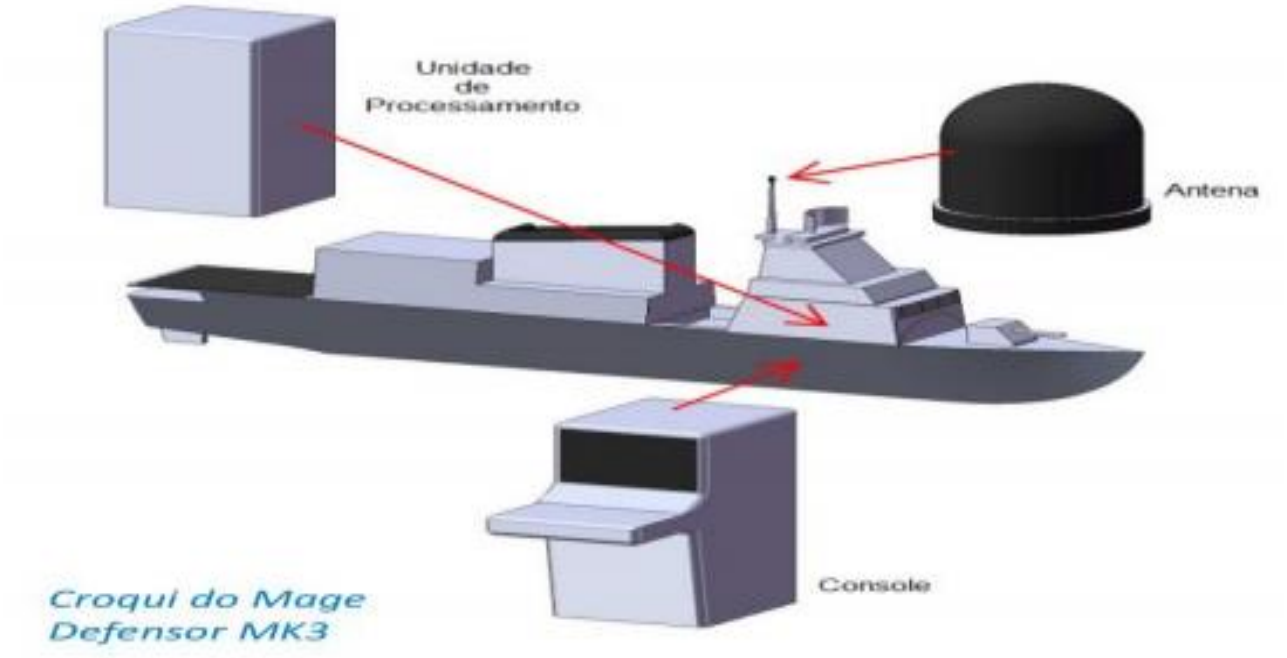
2.4.2 MAGE MK3

Visando o favorecimento da função do C^2, faz-se necessário a incorporação de novas funcionalidades aos equipamentos MAGE da MB, por isso, dentre os futuros equipamentos pode-se citar o MAGE MK3.

O MK3 será desenvolvido vislumbrando o aperfeiçoamento da aplicabilidade do MK2 e será instalado na Fragata Classe Tamandaré (FCT). O Sistema MAGE Defensor MK3 está sendo desenvolvido pelo IPQM e será instalado para identificar as emissões de radar em um determinado ambiente eletromagnético. O sistema consiste em unidades de antena, processamento de unidade e interface com operador (IOL) (ALVES, 2020).

O MK3 (Fig. 2.11) é um equipamento capaz de realizar o reconhecimento tático em um ambiente eletromagnético, possui um sensor capaz de interceptar radiações de emissores, a localização, o tempo de chegada e os parâmetros (largura de pulso, modulação intrapulso, amplitude, entre outros), frequência de repetição, varredura, radar envolvido e biblioteca de emissores. A Interface do equipamento implementa um ambiente gráfico, facilitando a visualização tática dos cenários das operações e do C^2. Além disso, acoplado ao equipamento, há um dispositivo de impressão de geração de relatórios em conformidade com o sistema, pois a biblioteca e o histórico das operações são realizados por intermédio de um disco flexível, uma memória flash e um CD-Room (GALANTE, 2018).

Figura 2.11: Croqui do MAGE MK3 das FCT.



Fonte: ALVES, 2020.

3. METODOLOGIA

Neste capítulo, será apresentado de forma metodológica o desenvolvimento e o processo de obtenção das informações obtidas para a construção deste trabalho.

3.1 Classificação da Pesquisa

Quando a Classificação da Pesquisa, a mesma decorre do embasamento dos fins, meios, limitações, coleta e qual foi o processo realizado a fim de obter as informações necessárias.

3.1.1 Quanto aos fins

Quanto aos fins, a pesquisa é classificada como descritiva e explicativa. Explicativa pois visa esclarecer as características sobre a GE e sua aplicabilidade diante do C². Descritiva, pois a pesquisa tende a abranger todos os conceitos, as finalidades e os subsídios.

3.1.2 Quanto aos meios

Quanto aos meios, a pesquisa consiste em uma revisão bibliográfica que visa a apresentação dos conceitos mencionados, pesquisando publicações cientificas e trabalhos anteriores, verificando todas as questões levantadas durante o trabalho.

3.2 Limitações do Método

Devido à diversidade da área do tema proposto, focou-se nos principais conceitos da GE, recursos e equipamentos disponíveis que tenham correlação com o C², não contendo especificidades de todos os métodos. Com isso, ressalta-se a necessidade de que seja feita uma abordagem analítica, baseada em trabalhos já existentes, em detrimento de uma pesquisa mais detalhada.

3.3 Coleta e Tratamento de Dados

Consistente com os dados citados nesta metodologia, este trabalho ainda se baseia na questão que norteia a pesquisa e prioriza outra forma de organização, que é aplicada a um banco de dados com um descritor específico. Sendo assim, esse processo foi organizado e separado em 2 etapas distintas, sendo elas:

Primeira etapa: Etapa em que ocorreu o estabelecimento e a identificação das questões norteadoras da pesquisa.

a) Pergunta de pesquisa 1: Como é a Guerra Eletrônica?
b) Pergunta de Pesquisa 2: Quais são as vertentes do Comando e Controle?
c) Pergunta de Pesquisa 3: Qual é a importância das informações aplicadas no C^2?
d) Pergunta de Pesquisa 4: Qual é a aplicabilidade de GE diante das vertentes que envolve o C^2?
e) Pergunta de Pesquisa 5: Quais equipamentos podem auxiliar o C^2 para a tomada de decisão?

Segunda Etapa: Etapa em que ocorreu a contemplação das publicações empregadas na construção deste trabalho. A pesquisa de busca foi aplicada nas seguintes bases de dados: Literatura Latino-americana e do Caribe em Ciências da Saúde (LILACS), na Biblioteca virtual *Scientific Electronic Library Online (Scielo)*, Google Acadêmico e *Naval Postgraduate School*.

Após empregar toda a metodologia de pesquisa apresentada, critérios de inclusão e exclusão foram inseridos a fim de favorecer e facilitar o direcionamento da pesquisa, sendo eles:

a) Critérios de Inclusão:

- Artigos publicados na língua portuguesa, inglesa e espanhola;
- Artigos publicados de 1990 a 2020;
- Trabalhos anteriores.

b) Critérios de Exclusão:

- Artigos pagos;
- Jornais;
- Artigos publicados em línguas que divergem a portuguesa, a espanhola e a inglesa;
- Artigos publicados fora do período estabelecido.

Desse modo, foram selecionadas publicações referentes à temática, sendo elas lidas e classificadas sequencialmente, integrando o presente trabalho e atendendo os critérios estabelecidos para a pesquisa.

4. DESCRIÇÃO E ANÁLISE DOS RESULTADOS

Em conformidade com o tema proposto, abaixo encontra-se uma análise *SWOT* apresentando quais são as forças, as fraquezas, as oportunidades e as ameaças da GE correlacionada ao C².

Tabela 4.1: Análise *Swot*.

ANÁLISE DE *SWOT*		
FATORES INTERNOS	**FORÇAS**	**FRAQUEZAS**
	- Utiliza Satélite como meio de comunicação; - Capacidade de adaptações e nacionalização de recursos tecnológicos; - Na MB, os sistemas de C^2 materializam a concepção de redução de custos; e - Emprego de Estratégias operacionais e táticas nas operações de GE.	- Disponibilidade de funcionalidades inúteis à aplicações militares; e - Emprego de satélites comerciais acarreta na elevação do custo operacional (VIVEIROS, 2007).
FATORES EXTERNOS	**OPORTUNIDADES**	**AMEAÇAS**
	- Avanços tecnológicos; - Treinamento e qualificação da equipe; e - Emprego de Software nas operações.	- Dependência de satélites; - Possibilidade de incompatibilidade dos softwares com o Sistema já integrado; e - Vulnerabilidade das informações.

Fonte: Elaborada pelo autor.

5. CONCLUSÃO

A informação é um bem de extrema importância e, proporciona inúmeros benefícios àqueles que a possuem. A capacidade de absorvê-la e processá-la, antecipadamente, durante as operações de guerra, beneficia o planejamento mais eficiente de um ataque. Além disso, ela permite desenvolver e utilizar novas ideias e metodologias, assim como empregar a tecnologia em favor de determinada operação.

Desse modo, no decorrer deste trabalho, foram apresentadas todas as conceituações necessárias sobre a GE e as suas ações, assim como as vertentes que se aplicam às funções do C². Através da análise apresentada foi possível observar a importância que a coleta da informação possui diante das ações do Comandante e da decorrência de uma GE.

Assim, pelos argumentos apresentados, a forma como o C² tem sido empregado é fator não apenas de sucesso nas operações, mas também, de fracasso e derrota no combate. A tarefa de empregá-lo com eficácia se revela, portanto, como um seguro indicador de competência na gerência do poder militar de uma nação

O C^2 demanda de informações imediatas e seguras durante uma operação para que as ordens e o direcionamento da missão possam ocorrer conforme as necessidades. As necessidades do C^2 são correlacionadas com a coordenação logística, visto que ele depende diretamente das informações coletadas, das ações de ataque e das medidas protetivas, o que remonta à aplicabilidade da GE.

A GE atua através da utilização do EEM, sendo esta utilização um requisito da comunicação via satélite. Através da atuação da GE, mediante as MPE, houve uma elevação na segurança da utilização dos recursos informacionais, e por essa razão, tais medidas de proteção passaram a ser utilizadas no processo de comunicação de C². Assim, de forma a compensar vulnerabilidades, é possível empregar as MPE para que o uso do espectro eletromagnético possa ser garantido por forças amigas, além de, mitigar as possiblidades e suscetibilidades de detecções de emissões de sinais considerando as MAE do inimigo.

Ademais, considerando uma perspectiva futura, a MB considera que, para se antepor às novas ameaças globais e tecnológicas é necessário conceder maior aplicabilidade às MPE. Em decorrência disso, a GE tornou-se um ponto de inflexão nas guerras modernas e investimentos, como o aprimoramento do MAGE Defensor para o MK3, que foram citados nesse trabalho, são necessários para esse setor, pois se trata de um equipamento formulado

tecnologicamente para substituir os obsoletos em face das novas necessidades da MB em relação às ações do C² e da GE.

5.1 Considerações Finais

Vale ressaltar que esta produção não esgota a possibilidade de pesquisa sobre a GE e o C², assim como as vertentes que envolvem a união das suas ações. Desse modo, tal completude não é mencionada no decorrer do trabalho, visto que não estão diretamente incluídas aos objetivos propostos.

5.2 Sugestões para Futuros Trabalhos

Almeja-se que após a apresentação desta temática novas pesquisas possam ser implementadas, visto a infinitude de abordagens que podem ser apresentadas, pois as vertentes que englobam a GE e a aplicabilidade do C² são amplas, principalmente ao que se diz respeito à Marinha do Brasil.

REFERÊNCIAS

ACÁCIO, G.J.S. **Integração das Forças Armadas Brasileiras**: uma análise da governança proporcionada pelos sistemas militares de Comando e Controle. 2018. 122f. Dissertação (Mestrado em Ciências Militares) – Escola de Comando e Estado – Maior do Exército, Rio de Janeiro, 2018.

ALVES, E. B. **MAGE MK3: O Futuro da Guerra Eletrônica na MB.** CIAW – Centro de Eletrônica, Comunicação e Segurança da Informação. 2020.

BELLINTANI, A.; BELLINTANI, M. **A Guerra: do século XIX aos nossos dias**. Boa Vista: Editora UFRR. 2014.

BORGES, G. A. **Sistema de Comando e Controle para a Amazônia Azul:** Adequabilidade, Exequibilidade e Aceitabilidade da Integração de Diversos Sistemas Independentes e Possíveis Alternativas. Monografia (Curso de Política e Estratégia Marítimas) – Escola de Guerra Naval, Rio de Janeiro, 2007.

BRASIL. Ministério da Defesa. **MD33-M-03 Doutrina Básica de Comando Combinado.** Brasília, DF, 2001.

_____. CENTRO DE INSTRUÇÃO DE GUERRA ELETRÔNICA - **Curso Básico de Guerra Eletrônica. Manual de Ensino de GE COM: nota de aula. Fase presencial.** Brasília, DF, 2013.

_____. Estado-Maior da Armada. **EMA-305 Doutrina Básica da Marinha**. 2. Rev. Brasília, DF, 2014a.

_____. Ministério da Defesa. Exército Brasileiro**. Caderno de Instrução EB70-CI-11.403 Medidas de Proteção Eletrônica**.1. ed. Brasília, DF, 2014b.

_____. Ministério da Defesa. **MD31-M-03 Doutrina Militar de Comando e Controle.** 3.ed. Brasília, DF, 2015a.

_____. Ministério da Defesa. **MD35-G-01 Glossário das Forças Armadas**. 5.ed. Brasília, DF, 2015b.

_____. Ministério da Defesa. Exército Brasileiro**. Manual de Campanha EB70-MC-10.201 A Guerra Eletrônica na Força Terrestre**.1. ed. Brasília, DF, 2019.

CESAR, W. C. **Uma história das Guerras Navais: o desenvolvimento tecnológico das belonaves e o emprego do poder naval ao longo dos tempos**. Rio de Janeiro – FEMAR. 2013.

COAKLEY, Thomas P. **Command and Control for War and Peace**. Diane Publishing, 1992.

DRISCOLL, D. E. HOWARD, S. F. **The Detection of Radar Pulse Sequences by Means of a Continuous Wavelet Transform.** IEEE Proceedings on International Conference Acoustics, Speech and Signal Processing, vol.3, p. 1389-1392, 1999.

GALANTE, A. **Jane's: NDM Bahia receberá MAGE Defensor Mk3**. SAAB. 2018. Disponível em: https://www.naval.com.br/blog/2018/12/19/janes-ndm-bahia-recebera-mage-defensor-mk3/. Acesso em: 03 de abr. de 2021.

GARCIA, P. R. G. et al. **Guerra de Informação: Conceituação Geral e Como Inseri-la na Marinha do Brasil**. Rio de Janeiro: Escola de Guerra Naval, 2005.

MAINI, A. K.; AGRAWAL, V. **Satellite technology: principles and applications**. 2nd. ed. Chichester: John Wiley & Sons LTD, 2011.

POISEL, Richard. **Modern communications jamming principles and techniques**. Artech House, 2011.

RICHARDSON, D. **Guerra eletrônica: guia das armas de guerra**. São Paulo: Nova Cultural. 1991.

SILVA, F. C. T. da. **A Guerra Assimétrica no Iraque**. 2009.

TZU, S. **A Arte da Guerra**. 35 ed. Rio de Janeiro: Record, 111 p. Tradução de: José Sanz. 2006.

UNITED STATES OF AMERICA. **Joint Publication 1-02: Dictionary of Military and Associated Terms**, JP 1-02. Washington, D.C.: United States Department of Defense, 597 p. 2001.

VIEIRA, A. M. **O avanço tecnológico e as novas habilidades do analista de GE.** Sentinela da Colina, n. 6, Brasília, DF: Centro Integrado de Guerra Eletrônica. 2008

VIVEIROS, C. P. **Fatores de Comando e Controle Aplicáveis nas Operações Combinadas.** O Sistema Militar de Comando e Controle. 2007. 68 f. Monografia (Curso de Política e Estratégia Marítimas) – Escola de Guerra Naval, Rio de Janeiro, 2007.