UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG

CURSO DE GESTÃO DE OPERAÇÕES E LOGÍSTICA

TRABALHO DE CONCLUSÃO DE CURSO

MATÍAS FERNANDO CAZÓN

Guerra Eletrônica em apoio à função de combate da Inteligência.

PÓS GRADUAÇÃO *LATO SENSU*

RIO DE JANEIRO, RJ
2023

TERMO DE AUTORIZAÇÃO DE USO E APROVAÇÃO

MATÍAS FERNANDO CAZÓN

GUERRA ELETRÔNICA EM APOIO À FUNÇÃO DE COMBATE DE INTELIGÊNCIA.

Autorizo que o presente artigo científico submetido ao Curso de Pós-Graduação *Lato Sensu* da A FURG, como requisito parcial para obtenção do certificado de Especialista em Gestão de Operações e Logística, e aprovado pelos docentes responsáveis pela orientação e sua aprovação, é utilizado para pesquisas acadêmicas de outros participantes deste ou de outros cursos, a fim de aprimorar o ambiente acadêmico em discussão em torno dos temas aqui propostos.

TÍTULO: GUERRA ELETRÔNICA EM APOIO À FUNÇÃO DE COMBATE DE INTELIGÊNCIA.
AUTOR: MATÍAS FERNANDO CAZÓN
CONSELHEIRO: PROF. JORGE TELLO GAMARRA

RESUMO

A Guerra Electrónica não é de facto nova, tem a sua origem na Guerra Russo-Japonesa (1904) embora no início tenha desempenhado um papel secundário nas operações militares, foi na Segunda Guerra Mundial (1939-1945) onde teve um papel relevante . A partir daí, a sua evolução esteve sujeita aos avanços tecnológicos e cada conflito onde foi utilizado gravitou o resultado para quem melhor aproveitou os seus benefícios. Atualmente faz parte de uma forma de realizar operações de apoio, enquadradas na Guerra de Informação, apoiando cada função de combate, mas principalmente a função de Comando e Controlo (C2) e a função de Inteligência. Na primeira, permite manter e aumentar a consciência situacional de um comandante e seu estado-maior em cena, e na segunda, há uma relação recíproca entre Inteligência e Guerra Eletrônica, onde uma depende da outra para poder desenvolver suas atividades em o campo de batalha. O objetivo deste artigo é destacar a relação que existe entre essas duas atividades e como elas contribuem para a consciência situacional do comandante. O método utilizado foi a revisão bibliográfica, tanto para caracterizar os fundamentos deste trabalho quanto para estabelecer as bases técnico-táticas de ambas as atividades analisadas. Os resultados obtidos foram dois, em primeiro lugar, a relevância da Guerra Electrónica no apoio à tomada de decisão através da sua relação com a Inteligência e Comando e Controlo, e em segundo lugar, a importância que tem para os decisores. grande importância para todos eles, pois contam com uma série de ferramentas que permitem realizar suas operações da forma mais eficiente possível.

PALAVRAS-CHAVE: Guerra Eletrônica, Inteligência, Consciência Situacional, Comando e Controle, Batalha.

TÍTULO DO TCC: GUERRA ELETRÔNICA EM APOIO À FUNÇÃO DE COMBATE DE INTELIGÊNCIA.

Matias Fernando Cazón

RESUMO -

A Guerra Electrónica não é de facto nova, tem a sua origem na Guerra Russo-Japonesa (1904) embora no início tenha desempenhado um papel secundário nas operações militares, foi na Segunda Guerra Mundial (1939-1945) onde teve um papel relevante . A partir daí, a sua evolução esteve sujeita aos avanços tecnológicos e cada conflito onde foi utilizado gravitou o resultado para quem melhor aproveitou os seus benefícios. Atualmente faz parte de uma forma de realizar operações de apoio, enquadradas na Guerra de Informação, apoiando cada função de combate, mas principalmente a função de Comando e Controlo (C2) e a função de Inteligência. Na primeira, permite manter e aumentar a consciência situacional de um comandante e seu estado-maior em cena, e na segunda, há uma relação recíproca entre Inteligência e Guerra Eletrônica, onde uma depende da outra para poder desenvolver suas atividades em o campo de batalha. O objetivo deste artigo é destacar a relação que existe entre essas duas atividades e como elas contribuem para a consciência situacional do comandante. O método utilizado foi a revisão bibliográfica, tanto para caracterizar os fundamentos deste trabalho quanto para estabelecer as bases técnico-táticas de ambas as atividades analisadas. Os resultados obtidos foram dois, em primeiro lugar, a relevância da Guerra Electrónica no apoio à tomada de decisão através da sua relação com a Inteligência e Comando e Controlo, e em segundo lugar, a importância que tem para os decisores. grande importância para todos eles, pois contam com uma série de ferramentas que permitem realizar suas operações da forma mais eficiente possível.

PALAVRAS-CHAVE: Guerra Eletrônica, Inteligência, Consciência Situacional, Comando e Controle, Batalha.

1 INTRODUÇÃO

A Guerra Eletrônica (GE) é um conjunto de atividades militares que utiliza a energia eletromagnética para enfraquecer o espectro eletromagnético do inimigo e proteger o nosso, onde o reconhecimento eletrônico, o ataque eletrônico e a proteção se incluem como ações principais (DONG YAN et al., 2022). Os campos de batalha hoje se tornaram mais dinâmicos do que há cem anos, hoje um comandante precisa saber em tempo real o que está acontecendo ao seu redor, o que estão fazendo seus elementos subordinados, unidades vizinhas e, principalmente, o adversário (BOYD, 2018). Ser capaz de antecipar ações com tempo suficiente para realizar seu ciclo OODA- *Observar, Orientar, Decidir e Agir* (BOYD, 2018).

Em 17 de janeiro de 1991 às 02h38, oito helicópteros AH-64 "*Apache*" atacaram dois radares de vigilância aérea iraquiana, minutos depois cinquenta e dois mísseis BGM-109 "*Tomahawk*" destruíram as principais defesas aéreas iraquianas. Às 02:50 daquele dia, aeronaves furtivas F-117 "*Nighthawk*" entraram no espaço aéreo iraquiano e atacaram o Centro de Informações de Combate (CIC) no oeste de Bagdá, outros caças Steel atacaram o Comando da Força Aérea e o Comando de Defesa Aérea inimigo, finalmente por volta das 3:00 a.m., quatro mísseis "*Tomahawk*" destruíram mais defesas aéreas iraquianas (SILVA, 2013). Não foram as aeronaves furtivas, mísseis de cruzeiro ou os mais recentes tanques e veículos mecanizados no solo que definiram com tanto sucesso a campanha da Coalizão, mas sim os sistemas de inteligência e guerra eletrônica disponibilizados aos comandantes da campanha (DESMOND BAL, 1991).

Embora a Guerra Eletrônica não seja recente, mas data do início do século XX, na guerra Russo-Japonesa de 1904 foi após a Segunda Guerra Mundial (1939-1945) que ela se tornou relevante e evoluiu até os dias de hoje como sabemos (ARCHANGELIS, 1983).

Mas por si só o GE não é nada, pelo contrário, faz parte de um sistema mais complexo onde, juntamente com outros elementos como Guerra Psicológica, Operações de Decepção, Operações de Segurança, contribuem para o que é chamado de Guerra de Informação (ou seu termo em inglês de *Information Warfare* (IW)) e que tudo isso contribui para a consciência situacional que um comandante

deve ter para tomar decisões em tempo hábil e com o maior detalhamento possível (TRAULLAS, 1998).

Atualmente, as pesquisas estão voltadas para permitir que aqueles que devem utilizar produtos de Inteligência e Guerra Eletrônica processem essas informações com mais rapidez, devido ao grande fluxo de dados que chegam a um centro de processamento (AL-KAWAJA, 2023). Exemplo disso é *Electronic Warfare Intelligence Information System* (EWIIS) cujo objetivo é facilitar o processamento de todos os dados que chegam dos diferentes sensores a um centro de informações de combate (AL-KAWAJA, 2023).

Nesse sentido, o objetivo deste artigo é descrever como a Guerra Eletrônica se relaciona com as funções de combate, e principalmente com as funções de combate Comando e Controle e Inteligência, sendo esta última a que terá mais peso específico ao receber as informações que vêm dos elementos para posteriormente processar essa informação e transmiti-la ao comandante para contribuir para a sua consciência situacional. Para tanto, o método proposto foi revisado na bibliografia.

Além da introdução, o estudo a seguir tem quatro seções. A seção 2 apresenta conceitos básicos da Guerra Eletrônica, sua origem, classificação, características e especificidades, a seção 3 apresenta a Inteligência Tática, a seção 4 apresenta a relação entre a Guerra Eletrônica e a Inteligência Tática. O artigo finaliza com a seção de considerações finais.

2 GUERRA ELETRÔNICA

2.1 Generalidades.

O espectro eletromagnético (EM) é uma área de manobra composta por todas as frequências de radiação eletromagnética (campos elétricos e magnéticos oscilantes caracterizados por frequência e compressão de onda) (ELECTRONIC WARFARE, 2012). O espectro eletromagnético é organizado em bandas de frequência com base em características físicas específicas (ELECTROMAGNETIC WARFARE TECHNIQUES, 2023).

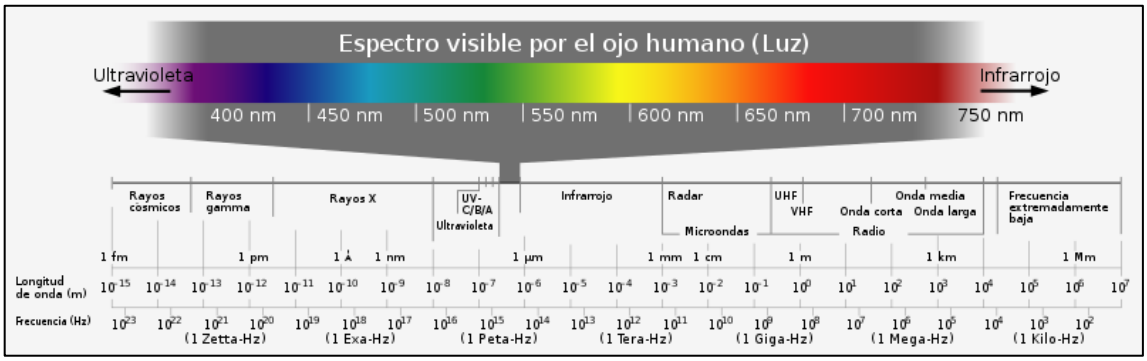
A guerra eletrônica pode então ser definida como a arte e a ciência de preservar ou usar o espectro eletromagnético para uso amigável enquanto nega seu uso ao inimigo (ADAMY, 2004). O espectro eletromagnético é claro de DC para luz (e

além). Portanto, a guerra eletrônica abrange todo o espectro de radiofrequência, ou espectro infravermelho, ou espectro óptico, e espectro ultravioleta (ADAMY, 2004).

2.2 Classificação.

O GE por sua vez tem sua divisão, isso é necessário porque neste tipo de operações podem ser realizadas diferentes tarefas e cada uma delas visa basicamente afetar (atacar) as emissões eletromagnéticas do inimigo, proteger nossas emissões e/ou contribuir (apoiar) com o GE as ações de outros elementos no campo de batalha (ELECTRONIC WARFARE-USMC, 2002).

Figura 1 Espectro eletromagnético



Fonte: Wikipedia (2023).

É importante compreender a intenção do comandante, coordenar, eliminar os conflitos e sincronizar as atividades de GE com outros elementos do estado-maior para aumentar a eficácia do combate, a proteção da força e sua projeção (ELECTROMAGNETIC WARFARE TECHNIQUES, 2023). Para isso, o GE divide-se, inicialmente, em três grandes atividades, a saber (BALL, 1991):

2.2.1 Suporte Eletrônico (AGE):

Apoio eletrônico é a divisão da guerra eletromagnética que envolve ações ordenadas por, ou sob o controle direto de, um comandante operacional para procurar, interceptar, identificar e localizar ou localizar fontes de energia eletromagnética irradiada intencional e não intencional para fins de reconhecimento gerenciamento de ameaças imediatas, direcionamento, planejamento e condução de operações futuras (ELECTRONIC WARFARE, 2012).

AGE (ou ES) difere de Inteligência de Sinais (SIGINT- *Signal Intelligence*) (compreendendo Inteligência de Comunicação (COMINT- *Communication*

Intelligence) e Inteligência Eletrônica (ELINT- *Electronic Intelligence*), embora todos esses campos envolvam o recebimento de transmissões inimigas cada vez mais vagos à medida que aumenta a complexidade dos sinais, estão nos propósitos para os quais as transmissões são recebidas (ADAMY, 2000).

- O COMINT recebe os sinais de comunicação do inimigo para extrair inteligência das informações transmitidas por esses sinais.
- O ELINT recebe sinais de não comunicação do inimigo para determinar os detalhes dos sistemas eletromagnéticos do inimigo para que contramedidas possam ser desenvolvidas. Portanto, os sistemas ELINT geralmente coletam muitos dados durante um longo período para fornecer informações e análises detalhadas.
- O AGE/ES, por outro lado, coleta os sinais do inimigo (seja comunicação ou não comunicação) para fazer algo imediatamente com os sinais ou as armas associadas a esses sinais. O sinal recebido pode ser bloqueado ou suas informações entregues a uma capacidade de resposta letal. Os sinais recebidos também podem ser usados para percepção situacional, ou seja, para identificar os tipos e a localização das forças, armas ou capacidade eletrônica do inimigo. O ESM/ES geralmente coleta muitos dados de sinal para suportar um processamento menos extenso com uma alta taxa de transferência. AGE/ES geralmente determina apenas qual dos tipos de emissores conhecidos está presente e onde eles estão localizados (ADAMY, 2000).

2.2.2 Ataque eletrônico (EA).

Ataque eletrônico é a divisão da guerra eletrônica que envolve o uso de energia eletromagnética, energia direcionada ou armas antirradiação para atacar pessoas, instalações ou equipamentos com a intenção de degradar, neutralizar ou destruir a capacidade de combate do inimigo e é considerado um ataque forma de fogo (ELECTRONIC WARFARE, 2012).

Os comandantes usam ataques eletrônicos para interromper as comunicações do adversário, bem como quaisquer sensores que o adversário possua no campo de batalha (ELECTRONIC WARFARE, 2012). Essas ações podem ser realizadas isoladamente ou como parte de outras ações sob o conceito de armas

combinadas, exemplo disso foi o que aconteceu em 1982 durante a Operação “Mole Cricket 19” realizada pela Força Aérea de Israel, cujo objetivo final era obter a superioridade aérea no sul do Líbano (JORDAN, 2012). Para alcançar essa superioridade aérea, os israelenses executaram um ataque aéreo coordenado com um ataque eletrônico às defesas aéreas sírias posicionadas ao longo do vale de Bekka (Líbano), onde primeiro com um ataque eletrônico de "jamming" eles perturbaram os sensores (radares) e bloquearam as comunicações inimigas para posteriormente bombardear os locais de mísseis antiaéreos sírios (MY CLARY, 1992).

A gama de atividades abrangidas pelo ataque eletrônico é ampla, podendo ser utilizadas individualmente ou em combinação (ELECTRONIC WARFARE, 2012).

- Interferir no radar ou nos sistemas de comando e controle do adversário;
- Empregue mísseis antirradiação para suprimir as defesas aéreas inimigas;
- Usando engano eletromagnético para confundir os sistemas de vigilância e reconhecimento do adversário;
- Use iscas autopropelidas, rebocadas ou estacionárias;
- Use medidas de autoproteção e proteção forçada, como o uso de consumíveis (flares e iscas ativas);
- Empregue energia direcionada ou contramedidas infravermelhas.

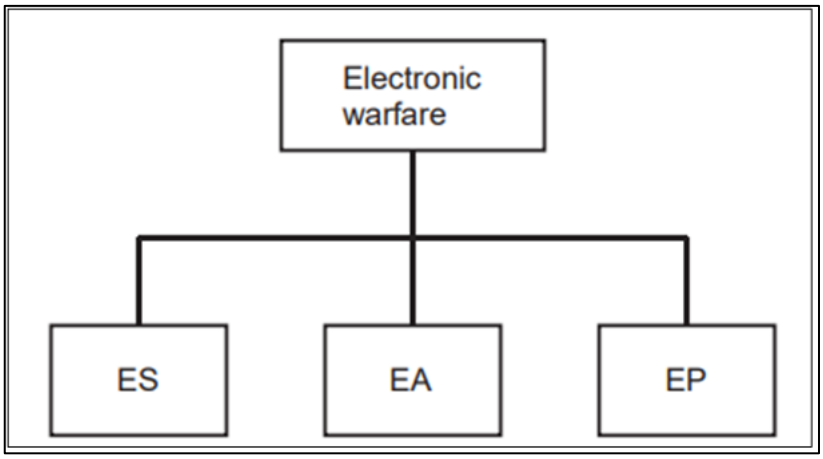
O ataque eletromagnético nega ao adversário o uso do espectro eletromagnético ou à sua equipa de utilização do referido espectro, procurando afetar a sua capacidade de comando e controlo, bem como a sua consciência situacional, obrigando-o a tomar decisões erradas ou intempestivas relativamente à atuação das nossas forças ou forças amigas. (ELECTRONIC WARFARE, 2012).

2.2.3 Proteção eletrônica (PE).

Proteção eletromagnética é a divisão da guerra eletromagnética que envolve ações tomadas para proteger pessoal, instalações e equipamentos de quaisquer

efeitos do uso amigo ou inimigo do espectro eletromagnético que degrada, neutraliza ou destrói a capacidade de combate amigo (ELECTRONIC WARFARE, 2012).

Figura 2 Classificação de Guerra Eletrônica



Fonte: ADAMY (2004).

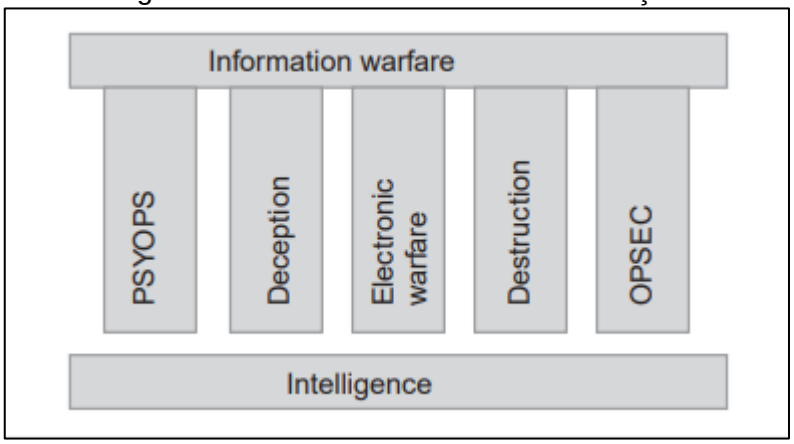
2.3 Características da Guerra Eletrônica.

As principais atividades de GE se desenvolveram ao longo do tempo para explorar as oportunidades e vulnerabilidades inerentes à física da energia EM. As principais atividades usadas no GE incluem o seguinte: contramedidas, gerenciamento de batalha EM (EMBM - *Electromagnetic Battle Management*), compatibilidade EM; engano EM; Endurecimento EM, resolução de bloqueio EM, intrusão EM, bloqueio EM, EMP (*pulso eletromagnético*), controle de espectro EM, coleta de inteligência eletrônica, mascaramento eletrônico, sondagem eletrônica, reconhecimento eletrônico, segurança eletrônica, reprogramação GE, controle de emissão, geolocalização de precisão e modos de espera em tempo de guerra (ELECTRONIC WARFARE, 2012).

Uma característica do GE que é parte integrante da chamada Guerra de Informação (IW- *Information Warfare*) (ALI AL-KHAWAJA; 2021). A guerra de informação inclui ações tomadas para preservar a integridade do sistema de informação de alguém contra exploração, interrupção do inimigo, enquanto ao mesmo tempo explora, corrompe ou destrói o sistema de informação de um adversário, bem como o processo de obtenção de uma vantagem de informação na aplicação da força (ADAMY, 2004). Os chamados pilares que compõem a Guerra de Informação são as Operações Psicológicas (PSYOPS), Engano, Guerra Eletrônica (GE), Destruição e

Operações de Segurança (OPSEC) (ADAMY, 2004). Todas essas atividades são baseadas na Inteligência, que é a função de combate que interage continuamente com cada uma delas, fornecendo feedback para fornecer ao comandante e seu estado-maior o que se chama de consciência situacional (TRAULLAS, 1998).

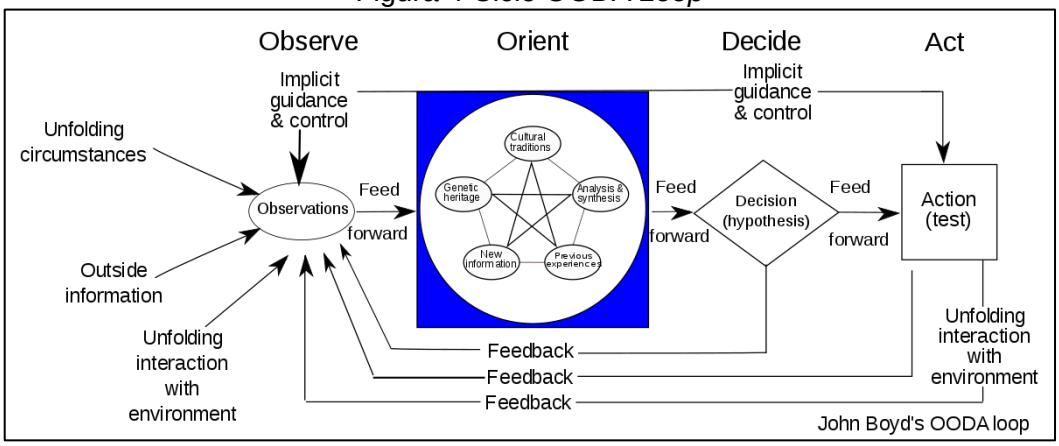
Figura 3 Estrutura da Guerra de Informação



Fonte: ADAMY (2004).

Essa consciência situacional permite o desenvolvimento mais eficiente da função de Comando e Controle (C2) de uma unidade no campo de batalha (MUNIR, 2022). Isso porque um comandante e seu estado-maior estão atualizados sobre tudo o que acontece com suas unidades próprias e amigas no terreno, bem como sobre a situação do inimigo em sua área de atuação (SILVA, 2019). É aí que entra o chamado ciclo OODA, tanto deles quanto do inimigo (SILVA, 2013). Este ciclo é composto por quatro etapas, Observação, Orientação, Decisão e Ação, foi idealizado pelo Coronel da USAF John Boyd na década de 1950 (Guerra da Coréia) e o que ele propõe é que ele (forças próprias ou adversário) realize mais ciclos OODA no menor tempo possível pode obter uma vantagem substancial sobre a outra parte e isso acaba marcando o sucesso do fracasso (KELLY, 2014)

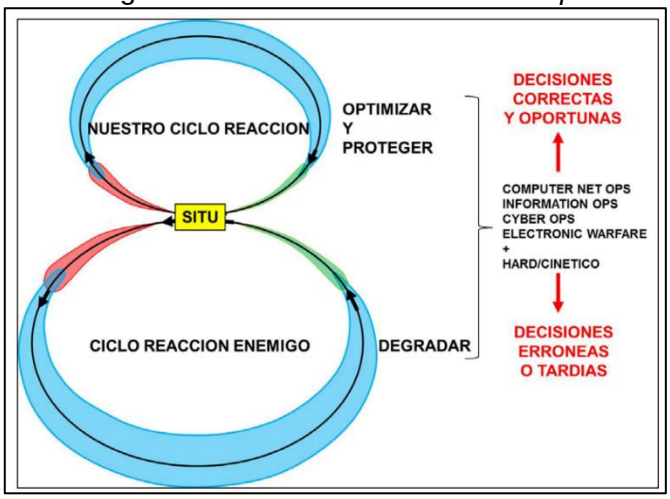
Figura 4 Ciclo OODA *Loop*



Fonte: www.laboneconsultoria.com.br.

O GE procurará contribuir para a consciência situacional do comandante e do seu estado-maior amigo, protegendo o espectro eletromagnético de qualquer interferência do adversário, ou seja, contribui para o desenvolvimento normal do seu próprio Ciclo OODA (SILVA, 2019). Enquanto isso, procurará perturbar ou negar o espectro eletromagnético do inimigo e, finalmente, seu ciclo OODA, distorcendo assim sua consciência situacional (SIVA, 2019).

Figura 5 A EW e o Ciclo OODA *Loop*



Fonte: SILVA (2019).

3 INTELIGÊNCIA

O que foi escrito há mais de seis séculos ainda é totalmente válido, para os exércitos ocidentais é considerada uma das seis funções de combate. O MCWP 2-10 *Operações de Inteligência* define inteligência como conhecimento do campo de batalha e das forças de ameaça (inimigas) neste espaço de batalha (MCWP 2-10, 2021). O conhecimento é gerado no apoio ao processo de tomada de decisão do

comandante e é resultado da coleta, processamento, exploração, avaliação, integração, análise e interpretação das informações disponíveis no campo de batalha e na ameaça (INTELLIGENCE OPERATIONS, 2021).

Em outras palavras, a inteligência refere-se ao aumento da consciência situacional do próprio lado, uma vez que é reduzida pelo lado do adversário (AL-KHAWAJA, 2021). A relevância deste conceito é explicada pelo MCDP-2 " *Intelligence* ", onde se destaca que a manobra de guerra requer um foco firme e não hostil. O objetivo é tomar medidas que contornem pontos fortes inimagináveis e explorem vulnerabilidades críticas. Identificar esses pontos fortes e vulnerabilidades é crucial (INTELLIGENCE-USMC, 2018). A guerra de manobras requer mover-se de forma a enganar e você deve atacar em um momento e local que o inimigo não espera e para o qual ele não está preparado (INTELLIGENCE-USMC, 2018). Também é importante identificar as expectativas e os preparativos do adversário. A guerra de manobras requer decisões e ações baseadas na consciência situacional: uma compreensão aguçada de dois fatores essenciais que tornam cada condição única, em vez de esquemas ou técnicas preconcebidas (INTELLIGENCE OPERATIOS, 2021).

Por outro lado, o Corpo de Fuzileiros Navais dos USA afirma que, para vencer no combate, os fuzileiros navais devem ser capazes de operar em ambientes instáveis e muitas vezes caóticos (WARFIGHTING, 1997). Uma guerra é um choque violento de vontades independentes, cada uma tentando colidir com a outra, criando atrito, incerteza, fluidez, desordem e complexidade. Essas características, combinadas com as várias dimensões da natureza humana, tornam a guerra uma atividade fundamentalmente imprevisível. A filosofia do Corpo de Fuzileiros Navais para ultrapassar estas condições assenta em manobras rápidas, flexíveis e oportunas. Conforme declarado no MCDP-1, "*Warfighting*", "a guerra de manobra é uma filosofia de guerra que busca destruir as forças inimigas por meio de uma variedade de ações rápidas, focadas e inesperadas que criam uma situação turbulenta e deterioração (WARFIGHTING, 1997). rapidamente com o qual o inimigo não pode lidar." A guerra de manobra requer manobras em vários domínios, não apenas tempo e espaço, para alcançar a superioridade sobre o inimigo (LIND, 1985). A guerra de manobra está concentrada em ações que representam o inimigo com uma série de dilemas em que os eventos se desenrolam inesperadamente e mais rápido do que o indivíduo pode

responder, é dizer, você está criando um dilema para o inimigo, onde a sua opção seja a que seja conlleva uma ventaja tatica favor das propias fuerzas (LIND, 1985).

3.1 Características da inteligência.

Como não há certeza absoluta na guerra, a “névoa” e o “atrito” não permitirão uma visão perfeita do ambiente operacional (INTELLIGENCE OPERATIONS, 2021). É por isso que a Inteligência deve trabalhar com todos os recursos à sua disposição para permitir que o comandante satisfaça suas necessidades de informação, e assim tenha maior consciência situacional e assim tome decisões com maior sucesso em cada etapa da operação que está ocorrendo (INTELLIGENCE OPERATIONS, 2021).

Nesse sentido, a Inteligência dispõe de diversos dispositivos implantados no campo de combate, todos eles com algum componente eletrônico (sensores) ou ligados a eles, onde são orientados para o inimigo, o terreno, o clima ou as condições meteorológicas da área de operações (AL-KHAWAJA, 2021).

É desenvolvido por meio de um processo chamado ciclo de inteligência, que é uma série de atividades relacionadas que traduzem a necessidade de inteligência sobre um determinado aspecto do campo de batalha ou ameaça em um produto baseado em conhecimento que é fornecido ao Comandante para uso no ciclo de tomada de decisão (INTELLIGENCE OPERATIONS, 2021).

Figura 6 CICLO DE INTELIGÊNCIA.

Intelligence Cycle	Key Considerations
Planning and direction	Plan intelligence operations and activities Support the commander in formulating an estimate of the situation
Collection	Develop the required intelligence structure Use organic, attached, and supporting intelligence sources to collect intelligence
Processing, exploitation, and production	Convert raw data and information into a suitable form of intelligence
Dissemination	Provide timely intelligence in an appropriate form to those who need it
Utilization	Use of intelligence

Fonte: MCWP 2-10 (2021).

As informações de inteligência (ou seja, informações usadas para gerar inteligência por meio do processo de análise) são geralmente extraídas de três tipos de dados: dados de inteligência, dados de sensores e dados de combate. (INTELLIGENCE OPERATIONS, 2021).

- Os dados de inteligência são derivados de ativos envolvidos principalmente na coleta de inteligência (por exemplo, imagens, interceptação eletrônica, fontes de inteligência humana - HUMINT);

- Os dados do sensor são derivados de sistemas tripulados e não tripulados usados para reconhecimento, vigilância ou aquisição de alvos (por exemplo, radar de vigilância aérea, radar de contrabateria, radar em sistemas de aeronaves não tripuladas (ARP), sensoriamento remoto do solo);

- Os dados de combate são derivados de relatórios de unidades subordinadas, adjacentes ou outras unidades aliadas.

O processamento de dados e informações em inteligência pode ser alcançado rapidamente em todos os níveis (INTELLIGENCE, 2018).

Os tomadores de decisão requerem conhecimento (inteligência útil, focada e avaliada) para aprimorar sua compreensão situacional. O ciclo de inteligência funciona continuamente para preencher lacunas de conhecimento e confirmar ou refutar informações fragmentadas. O processo está completo somente quando o conhecimento relevante foi aplicado para comandar a tomada de decisão. (INTELLIGENCE OPERATIONS, 2021).

4 MÉTODO.

Este trabalho utilizou como método a pesquisa exploratória, guiada por uma revisão bibliográfica, explorando as contribuições que outros autores deram ao tema da pesquisa. Posteriormente, uma sistematização dessas informações é apresentada nas seções resultados e análise de resultados.

Assim, a princípio, Guerra Eletrônica e Inteligência foram descritas separadamente, por outro lado, com o objetivo de entender como cada uma delas funciona, para depois descrever como elas se integram e funcionam de forma coordenada, alimentando-se mutuamente.

Por fim, nas considerações finais, será apresentado como ambas as atividades (Guerra Eletrônica e Inteligência) impactam no processo decisório de um

comandante e, ao mesmo tempo, como servem aos demais atores de uma organização para aumentar a consciência situacional de todos eles e assim aumentar as chances de antecipar as ações do adversário e assim obter uma vantagem sobre eles.

5 GUERRA ELETRÔNICA EM APOIO À FUNÇÃO DE COMBATE DE INTELIGÊNCIA.

Inteligência de todas as fontes são "produtos de inteligência e organizações e atividades que incorporam todas as fontes de informação, na maioria das vezes incluindo inteligência de recursos humanos, inteligência de imagem, inteligência de medição e assinatura, inteligência de sinais e dados de código. abertos na produção de inteligência final" (AL-KHAWAJA, 2021). Nesse sentido, a Guerra Eletrônica utiliza todos os recursos disponíveis para atender aos requisitos de Inteligência, através de suas três atividades principais, mas principalmente o suporte da guerra eletrônica com suas variáveis (SILVA, 2013).

O objetivo das atividades de Guerra Eletrônica de apoio à Inteligência, ambas como parte de um sistema maior denominado guerra de informação, é dar segurança aos tomadores de decisão ao garantir liberdade de ação em suas atribuições e degradar a capacidade do inimigo de fazer ações erradas ou tardias decisões sobre a situação que se apresenta naquele momento (TRAULLAS, 1998).

Figura 7 OTIMIZAR, PROTEGER, REBAIXAR.

Fonte: SILVA (2019).

Para conseguir isso, a Guerra Eletrônica usa os seguintes procedimentos no espectro eletromagnético (AL-KHAWAJA, 2021):

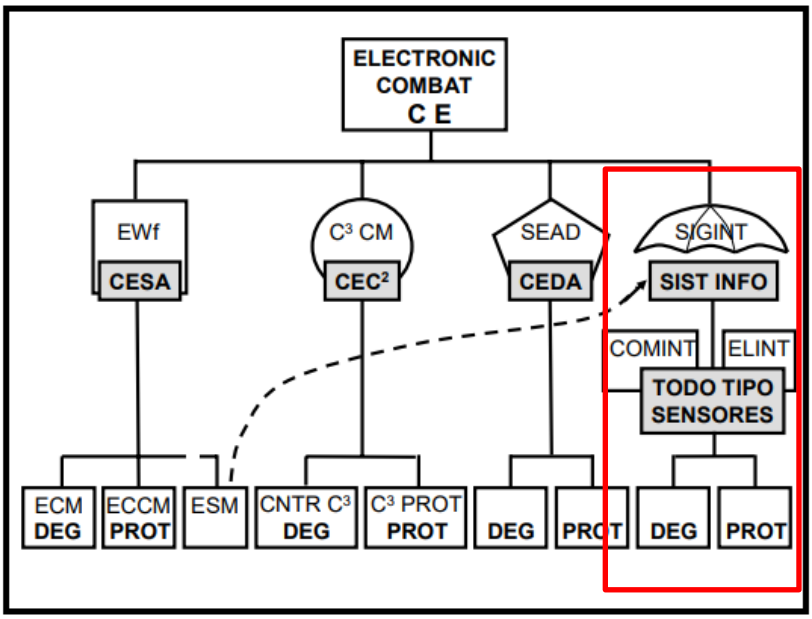
Inteligência de Sinais (SIGINT): É utilizada em nível estratégico e é definida como aquela atividade que busca obter informações a partir dos sinais emitidos pelo adversário, diferenciando-se do Suporte Eletrônico por estar em um nível superior a este (SILVA, 2013).

Inteligência de Comunicações (COMINT): É uma subdivisão da SIGINT e suas atividades visam proteger suas próprias emissões de comunicação e degradar as emissões de comunicação do adversário (SILVA, 2013).

Inteligência Eletrônica (ELINT): Subdivisão do SIGINT que direciona suas atividades para proteger as emissões que não são do seu tipo de comunicação e degradar as emissões que não são do tipo de comunicação do adversário (SILVA, 2013).

A imagem 8 é um gráfico melhor onde cabe o descrito acima.

Figura 8. SIGINT DENTRO DA GE.



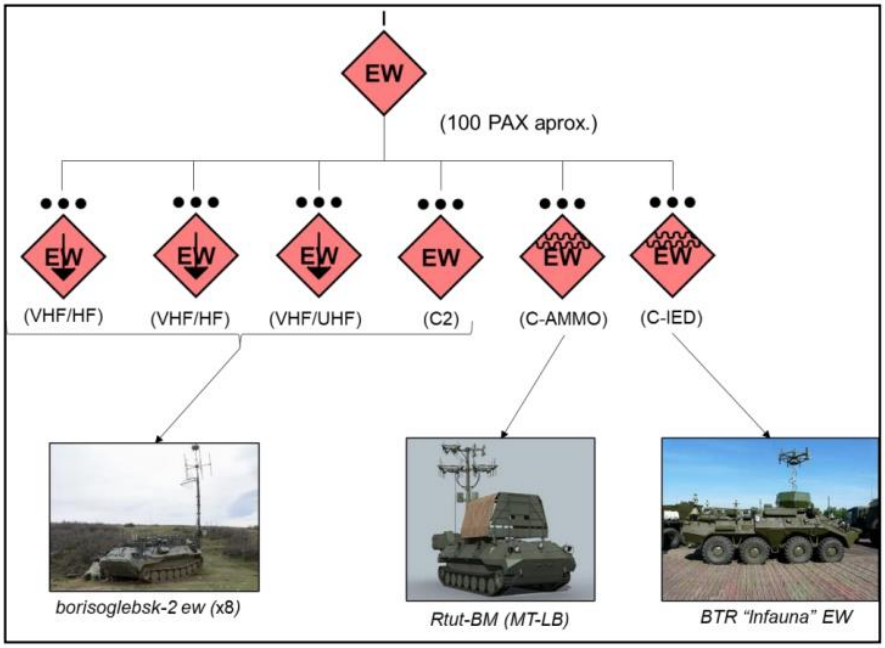
Fonte: SILVA (2013).

A relação que existe entre essas duas atividades é recíproca, ou seja, a Inteligência disponível é necessária para orientar os esforços da Guerra Eletrônica e, por sua vez, os dados obtidos da Guerra Eletrônica são necessários para alimentar o sistema de Inteligência de uma organização de combate (SILVA, 2019). Atualmente,

essa relação está cada vez mais presente em cada operação que as forças de um exército realizam, com a crescente dependência de sistemas de comunicação, sistemas de posicionamento, controle de armas e sensores que monitoram o campo de batalha, entre outros benefícios que a tecnologia coloca à disposição de um comandante (AL-KHAWAJA, 2021).

Recentemente, e num exemplo claro do que foi dito até agora, o Exército do Povo Chinês implantou uma série de instalações de inteligência de sinal que têm capacidade para realizar localizações rádio de localização em uma vasta região de sua área de influência, o Mar da China (AL-KHAWAJA, 2021). Outro país que viu a necessidade de organizar e equipar suas unidades terrestres com sistemas de Guerra Eletrônica foi a Rússia, desde a extinta União Soviética até os dias atuais (MONTOJO, 2019). Até o ano de 2003, o Exército Russo havia organizado suas unidades de GE em empresas que dependiam diretamente das Brigadas do Exército, bem como nas unidades de Infantaria de Fuzileiros Navais, desta forma, as grandes unidades de combate foram dotadas da capacidade de GE que permitia aos comandantes de brigada satisfazer suas necessidades de comando e controle e principalmente no apoio à Inteligência dessas unidades (MONTOJO, 2019).

Figura 9. Orgânica de um Ca. GE do Exército Russo.



Fonte: MONTOJO (2019).

6 GUERRA ELETRÔNICA E INTELIGÊNCIA NAS OPERAÇÕES DO CORPO DE FUZILEIROS NAVAIS.

Conforme já mencionado no ponto anterior, a Guerra Eletrônica e a Inteligência buscam dar segurança aos tomadores de decisão em todos os níveis da condução das operações militares (TRAULLAS, 1998). E isso é mais necessário hoje devido às diferentes variáveis que se apresentam no campo de batalha (PEREIRA et al, 2021). O US ARMY define esse ambiente com o acrônimo VUCA (*Volatility, Uncertain, Complex and Ambiguous*), introduzido na década de 1980 no final da Guerra Fria para definir as constantes mudanças nos ambientes assimétricos que as forças dos EUA tiveram que enfrentar (DIAZ, 2020). Neste ambiente cada vez mais complexo que não só as forças americanas devem enfrentar, é necessário ter o maior fluxo de informações e a maior confiabilidade possível e o mais rápido possível para que o próprio ciclo OODA supere o do adversário (SIVA, 2019) . É aqui, onde a Guerra Eletrônica desempenha um papel relevante na proteção das comunicações, vigilância e busca do espectro eletromagnético, e até ataques eletrônicos às capacidades do inimigo (SILVA, 2013).

Figura 10. Ambiente VUCA.

Performance Demands of a VUCA world		
Volatility	sudden change requires a rapid response; well-honed skills are easier to deploy	**Speed**
Uncertainty	inability to know for sure what will happen requires patience and a contingency plan	**Flexibility**
Complexity	many distinct but interconnected variables requires a broad range of response options	**Breadth**
Ambiguity	circumstances with multiple meanings require objectivity, without projecting biases	**Self-awareness**

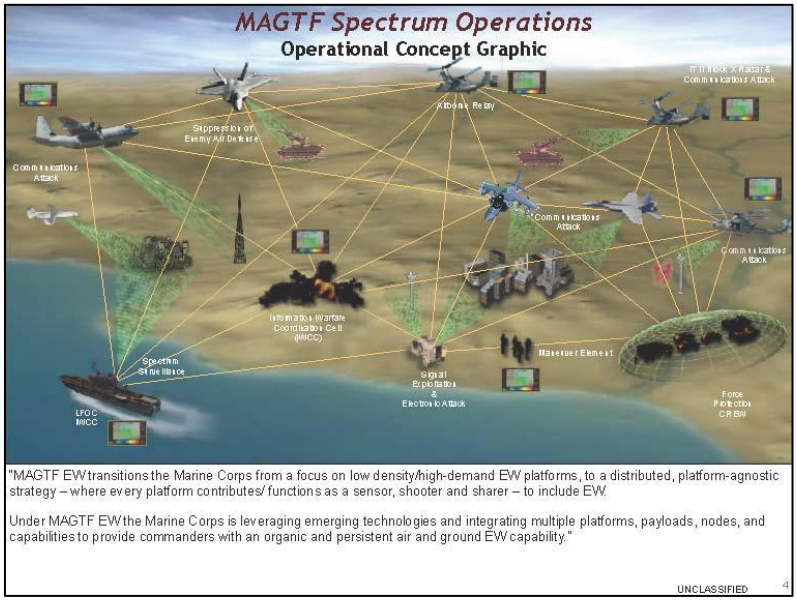
Fonte: LINKENDIN (2021).

Nas Operações Anfíbias, particularmente, esse tipo de ambiente impera nas situações em que uma Força de Pouso deve atuar (WARFIGHTING, 1997). Uma particularidade deste tipo de operações é que parte de um zero inicial de Poder de Combate no terreno e isso vulnera muito as forças no terreno nos primeiros momentos das operações (OPERACIONES ANFIBIAS, 2020). É por isso que ter uma

Inteligência capaz de antecipar os eventos que o ambiente operacional e o adversário apresentam às nossas forças, e a Guerra Eletrônica tem um papel relevante nas fases iniciais das operações anfíbias (ELECTRONIC WARFARE, 2012). Inicialmente, isso é feito com as informações disponibilizadas pela Força de Desembarque, são as informações que foram coletadas pelas unidades de Guerra Eletrônica durante o período em que não houve confronto (SILVA, 2013). Com essas informações, as unidades de Guerra Eletrônica direcionarão seus esforços para os sinais que já são conhecidos, ratificarão ou retificarão esses sinais e, por sua vez, reconhecerão novas emissões que o adversário fizer durante a chegada da Força-Tarefa Anfíbia ao Area do Objetivo Anfíbio (ELECTRONIC WARFARE, 2012).

Todos aqueles dados que as unidades do GE realizam antes da execução do Assalto Anfíbio servirão à Inteligência da Força de Desembarque para gerar as informações necessárias para transmitir aos tomadores de decisão para que possam realizar o planejamento mais preciso possível e consequentemente uma execução com o menor grau de incerteza (AMPHIBIOUS OPERATIONS, 2014).

Figura 11. Conceito Operacional do USMC.



Fonte: ROBBIN LAIRD (2017).

Antes de prosseguir, é necessário fazer uma distinção entre as ações que as unidades de GE realizam quando executam tarefas de Apoio à Guerra Eletrônica e aquelas realizadas por unidades de apoio à Inteligência (SILVA, 2013). As ações de Apoio à Guerra Eletrônica (AGE) e as ações de Inteligência de Sinais (SIGINT) se

distinguem devido a quem são direcionados os dados resultantes dessas ações, ou seja, os mesmos meios são utilizados para ambas as tarefas, mas recebem nomes diferentes. agência que o requer (ELECTRONIC WARFARE, 2012). Isso é importante destacar porque os mesmos meios são usados para ambas as ações, mas as informações obtidas serão processadas de forma diferente (SILVA, 2013).

A Guerra Eletrônica nas operações do Corpo de Fuzileiros Navais interage com outras atividades dentro do conceito de Guerra de Manobra e tem como principal missão interromper e degradar a capacidade do adversário de conduzir suas forças no campo de batalha (ELECTRONIC WARFARE, 2012). Além das outras tarefas (Suporte e Proteção), na Guerra de Manobras o objetivo será colocar o adversário em um dilema com seu ciclo OODA interrompido e suas forças no terreno desorientadas (LIND, 1985). Foi o que aconteceu em 1991 durante as primeiras horas da Operação *Desert Storm*, onde a Coalizão buscou descerebrar o adversário (Iraque) para deixar as forças desdobradas sem cabeça e sem condições de coordenar suas ações (SILVA, 2013). Ou o mesmo ocorrido anos antes, em 1982 durante a Operação Paz para a Galileia onde as Forças de Defesa de Israel realizaram uma operação aérea apoiada por unidades de Guerra Eletrônica para garantir o espaço aéreo e assim acompanhar as forças terrestres (MY CLARY, 1992).

Em ambos os casos, o objetivo era o mesmo de degradar a capacidade do adversário para que ele pudesse tomar decisões corretas e oportunas, e em ambos os casos a Guerra Eletrônica teve papel preponderante (SILVA, 2019). Mas essas ações não teriam sido realizadas se não houvesse a participação da Inteligência, em cada etapa das operações desde o início do planejamento até a execução e verificação dos resultados dessas ações (SILVA, 2019).

Figura 12. GE no processo de tomada de decisão do inimigo.

Fonte: ADAMY (2004).

Em Operações Anfíbias será muito difícil para o Comandante da Força de Desembarque ter o controle das operações de Guerra Eletrônica inicialmente (ELECTRONIC WARFARE, 2012). É por isso que o Comandante da Força-Tarefa Anfíbia será responsável por este tipo de operações, pelo menos até que a Força de Pouso esteja instalada no terreno com todos os seus componentes de Comando e Controle necessários para assumir, parte das operações de Guerra Eletrônica, principalmente aquelas que afetam diretamente a Força de Desembarque (ELECTRONIC WARFARE-USMC, 2002).

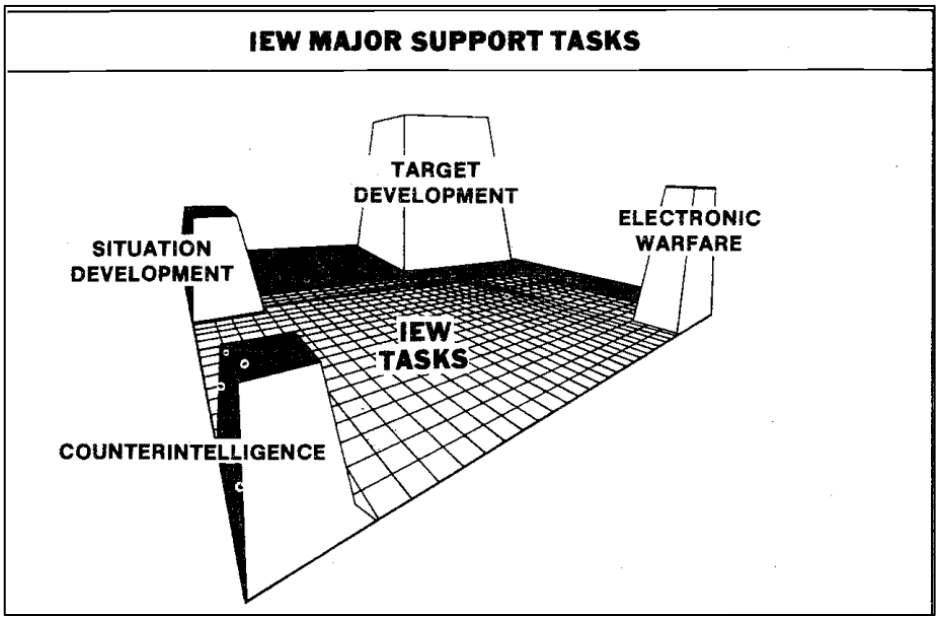
Para degradar as capacidades de comando e controle do adversário, as primeiras unidades a desembarcar serão aquelas que executam tarefas de Suporte de Guerra Eletrônica (AGE), pois devem localizar as emissões do inimigo e uma vez nos centros de comando e controle e após um processo de Inteligência, o as informações disponíveis aos tomadores de decisão permitirão que eles realizem as ações necessárias para perturbar o espectro eletromagnético do inimigo (GUERRA ELETRÔNICA-USMC, 2002).

A próxima coisa que será feita será planejar e executar Ataques Eletrônicos (AE) nessas emissões, a fim de cortar o ciclo OODA do adversário (SILVA, 2013). Nesse ponto, o Comandante da Força de Desembarque deve ter informações atualizadas sobre a situação dentro de sua zona de ação para fazer uso eficiente dos

poucos meios de Guerra Eletrônica de que dispõe (ELECTRONIC WARFARE-USMC, 2002).

As ações de Proteção Eletrônica (EP) devem estar ativas em todos os momentos para garantir a liberdade de ação no uso do espectro eletromagnético, especialmente nos momentos em que diferentes unidades estão operando em estreita proximidade ou em suporte mútuo (ELECTRONIC WARFARE-USMC, 2002).

Figura 13. Relação entre GE e inteligência.



Fonte: FM 34-10 DIV. INTELLIGENCE AND EW OPERATIONS (1986).

7 CONSIDERAÇÕES FINAIS

Conforme será afirmado no ponto 4 (Método), o artigo buscou inicialmente descrever a Guerra Eletrônica e a Inteligência separadamente para posteriormente descrever como ambas as atividades se complementam para apoiar a tomada de decisão que um comandante em campo deve fazer, desde o início do planejamento até a execução das operações.

Inicialmente, como primeira contribuição deste artigo, foi possível citar a relevância que a Guerra Eletrônica se evidencia hoje para satisfazer as necessidades das diferentes funções de combate, mas principalmente nas funções de Comando e Controle e Inteligência de combate. O artigo descreveu as principais tarefas que são executadas pelo GE, suporte, ataque e proteção.

Evidenciou-se a relevância da função de combate da Inteligência, sendo entendida como uma atividade gravitante para a consciência situacional dos tomadores de decisão no nível tático. Além disso, como busca manter atualizado o conhecimento situacional dos comandantes no campo de batalha, utilizando diferentes fontes dentro e fora da área de operações, seja em tempo de paz ou quando o conflito está ocorrendo.

Por fim, foi descrita a integração de ambos os conceitos (GE e Inteligência), sendo o primeiro uma atividade contributiva para o segundo e a reciprocidade que existe entre eles. Sempre direcionando o esforço principal de ambos para permitir que os tomadores de decisão funcionem da forma mais assertiva possível em um ambiente cada vez mais ambíguo como os cenários atuais. É neste aspecto que se menciona como respondem estas atividades nas operações da Infantaria de Fuzileiros Navais, principalmente nas Operações Anfíbias. Lembrando que este tipo de operações não só parte de um zero inicial de poder de combate no terreno, mas que isso faz com que os comandantes tenham pouca informação sobre o que acontece no terreno nos momentos iniciais das operações e que é tarefa de primeira prioridade da Inteligência Tática esclarecer a situação que se apresenta. E neste aspecto, a Guerra Eletrônica desempenha um papel importante desde o início, principalmente nas tarefas do GECOM (Guerra Eletrônica de Comunicações).

Com o exposto, busca-se que aqueles que têm a responsabilidade de tomar decisões nas organizações militares considerem os aspectos aqui levantados como uma necessidade imperante na atualidade. Sabe-se que ter organizações capazes de realizar tanto atividades de GE quanto de Inteligência requer um investimento monetário significativo, pois essas atividades são de alta demanda por tecnologia de ponta e isso para as forças armadas de países como os latino-americanos torna-se um item difícil de satisfazer. Mas que é preciso ter pelo menos um mínimo de capacidade, que permita aos futuros comandantes terem a capacidade de visualizar a situação que se apresenta e agir antecipadamente.

Naturalmente, este artigo não tentou cobrir todos os tópicos que ambas as atividades possuem, considerando que seu escopo se limita a descrever conceitos já desenvolvidos e expor questões que são atuais hoje. Mas pode ser um ponto de

referência para trabalhos futuros no campo da integração dos conceitos de Guerra Eletrônica e Inteligência.

REFERÊNCIAS

DONG YAN, et al, Research on the Construction of a Fifth-Dimensional Battlefield Base on UAVs- Integrated Electronic Warfare System to Size Electronic Magnetic Rights; Mechatronics and Automation Technology J. Xu (Ed.); 2022.

JHON R. BOYD, A Discourse on Winning and Losing, Alabama: Air University Press, 2018.

MIGUEL ANGEL SILVA, Al Enemigo Primero lo Descerebramos, Buenos Aires: RESGA, 2013.

DESMOND BALL, The Intelligence War in the Gulf, Canberra: Australian National University, 1991.

MARIO DE ARCANGELIS, Historia de la Guerra Electrónica, Madrid: San Martín, 1983.

JESÚS TRAULLAS, Concepto y fuentes para el estudio de la Information Warfare (pág. 185-192), Revista de la Universidad de Murcia Vol. I: España, 1998.

UNITED STATE ARMY. Electromagnetic Warfare Techniques (ATP 3-12.3), Washington D.C.: US Army, 2023.

DAVID L. ADAMY, EW 102 A Second Course in Electronic Warfare, Boston: Arteche House, 2004.

JOINT CHIEFS OF STAFF, Electronic Warfare (JP 3-13.1), Washington D.C, 2012.

UNITED STATE MARINES CORPS, Intelligence (MCDP 2), Washington D.C: Headquarters USMC, 2018.

UNITED STATE MARINES CORPS, Intelligence Operations (MCWP 2-10), Washington D.C: Headquarters USMC, 2021.

UNITED STATE MARINES CORPS, Electronic Warfare (MCWP 3-40.5), Washington D.C: Headquarters USMC, 2002.

ALI AL-KHAWAJA, et al; Intelligence and Electronic Warfare: Challenges and Future Trends; ICCITM, Mosul, 2021.

MIGUEL ANGEL SILVA; El Sistema de Información, Buenos Aires: UNDEF, 2019.

MARK KELLY, The OODA Loop: Applying Military Strategy to High-Risk Decision Making and Operational Learning Processes for On-Snow Practitioners; AMGA; 2014.

MUNIR, ARSLAN et al; Situational Awareness: Techniques, Challenges, and Prospects; Ed. Rüdiger Buchkremer; 2022.

UNITED STATE MARINES CORPS, Warfighting (MCDP 1), Washington D.C: Headquarters USMC, 1997.

WILLIAMS LIND, Maneuver Warfare Handbook, Colorado: Westview Press Inc., 1985.

RICARDO PEREIRA et al, Competências do Líder em um Mundo Vuca: Uma Revisão de Escopo, Convibra, 2021.

BENITO ANDRÉS ALLENDES DÍAZ, Entorno VUCA: Enfrentando el Desafío Organizacional a Través del Liderazgo Efectivo, Universidad del Desarrollo, Facultad de Ingeniería, Santiago de Chile, 2020.

ARMADA ARGENTINA, Operaciones Anfibias (R.O-2-099), Puerto Belgrano, 2020.

JOINT CHIEFS OF STAFF, Amphibious Operations (JP 3-02), Washington D.C, 2014.

MY DAVIS E. CLARY, Guerra Electrónica en el Valle de Bekka: Una nueva perspectiva (pág. 39-50), Military Review Vol. LXXII, 1992.

JAVIER JORDÁN, Drones israelíes en el valle de Bekka. Disponível em: <https://global-strategy.org/drones-israelies-batalla-valle-bekaa>, Acesso em: 23 jul. 2023, 11:00:00.

FERNANDO MANRIQUE MONTOJO, Panorama de la Guerra Electrónica en Rusia, Madrid: Instituto Español de Estudios Estratégicos, 2019.