ACADEMIA MILITAR DAS AGULHAS NEGRAS
ACADEMIA REAL MILITAR (1811)
CURSO DE CIÊNCIAS MILITARES

Otávio Prochmann Loebens

A GUERRA ELETRÔNICA NOS CONFLITOS ATUAIS E SEUS REFLEXOS PARA O EXÉRCITO BRASILEIRO

Resende
2023

TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL

TÍTULO DO TRABALHO: A GUERRA ELETRÔNICA NOS CONFLITOS ATUAIS E SEUS REFLEXOS PARA O EXÉRCITO BRASILEIRO
AUTOR: OTÁVIO PROCHMANN LOEBENS

Este trabalho, nos termos da legislação que resguarda os direitos autorais, é considerado de minha propriedade.

Autorizo a Academia Militar das Agulhas Negras (AMAN) a utilizar meu trabalho para uso específico no aperfeiçoamento e evolução da Força Terrestre, bem como a divulga-lo por publicação em período da Instituição ou outro veículo de comunicação do Exército.

A Academia Militar das Agulhas Negras poderá fornecer cópias do trabalho mediante ressarcimento das despesas de postagem e reprodução. Caso seja de natureza sigilosa, a cópia somente será fornecida se o pedido for encaminhado por meio de uma organização militar, fazendo-se a necessária anotação do destino no Livro de Registro existente na Biblioteca.

É permitida a transcrição parcial de trechos do trabalho para comentários e citações desde que sejam transcritos os dados bibliográficos dos mesmos, de acordo com a legislação sobre direitos autorais.

A divulgação do trabalho, em outros meios não pertencentes ao Exército, somente pode ser feita com autorização do autor ou do Diretor de Ensino da AMAN.

Resende, 31 de maio de 2023.

Cad Otávio Prochmann **Loebens**

Dados internacionais de catalogação na fonte

L825g LOEBENS, Otávio Prochmann
A guerra eletrônica nos conflitos atuais e seus reflexos para o Exército Brasileiro / Otávio Prochmann Loebens – Resende; 2023. 46
p. : il. color. ; 30 cm.

Orientador: Renan Viana Rocha
TCC (Graduação em Ciências Militares) - Academia Militar dasAgulhas Negras, Resende, 2023.

1. Guerra eletrônica. 2. Espectro eletromagnético. 3. Conflitos. 4.Exército Brasileiro. I. Título.

Ficha catalográfica elaborada por Aline Viegas da Costa CRB-7/7409

Otávio Prochmann Loebens

A GUERRA ELETRÔNICA NOS CONFLITOS ATUAIS E SEUS REFLEXOS PARA O EXÉRCITO BRASILEIRO

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares.**

Orientador: 1° Ten Com Renan Rocha.

Resende
2023

Otávio Prochmann Loebens

A GUERRA ELETRÔNICA NOS CONFLITOS ATUAIS E SEUS REFLEXOS PARA O EXÉRCITO BRASILEIRO

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares.**

Aprovado em 18 de agosto de 2023.

Banca Examinadora:

Renan Viana Rocha, 1º Tenente
(Presidente/Orientador)

Daniel do Amaral Pereira, Major
(Avaliador)

Tiago Santos de Sousa, 1º Tenente
(Avaliador)

Resende
2023

RESUMO

A GUERRA ELETRÔNICA NOS CONFLITOS ATUAIS E SEUS REFLEXOS PARA O EXÉRCITO BRASILEIRO

AUTOR: Otávio Prochmann Loebens
ORIENTADOR(A): Renan Viana Rocha

A guerra eletrônica é fator fundamental nos conflitos militares atualmente. O controle do espectro eletromagnético proporcionam grandes vantagens e aumenta as chances de sucesso para quem o possuir. Este trabalho tem como objetivo analisar a utilização do espectro eletromagnético e a importância em possuir a soberania nesse meio, tendo como base alguns equipamentos de guerra gletrônica empregados pelo Exército Russo e pelo Exército Americano e como foram utilizados em alguns conflitos, como a Guerra do Golfo, a Guerra da Síria e a Guerra Russo-Ucraniana. Além disso, ainda procura evidenciar ensinamentos retirados desses conflitos e como afetam o Exército Brasileiro. Por meio de pesquisas bibliográficas e documentais, foram demonstrados sistemas de guerra eletrônica russos e americanos e acontecimentos envolvendo esses sistemas em conflitos atuais. A justificativa deste trabalho sedá pela necessidade em compreender como a guerra eletrônica pode influenciar fortemente os resultados de um conflito, evidenciando as capacidades e limitações das grandes potências mundias nesse ramo, de forma a apresentar resultados que possam melhorar as capacidades da guerra eletrônica do Exército Brasileiro. Foi possível concluir que o Brasil necessita investir mais recursos em material, doutrina e capacitação pessoal para que seja possível acompanhar as constante evoluções tecnológicas na guerra eletrônica.

Palavras-chave: Guerra eletrônica. Espectro eletromagnético. Exército Brasileiro. Conflitos.

ABSTRACT

ELECTRONIC WARFARE IN CURRENT CONFLICTS AND ITS REFLECTIONS FOR THE BRAZILIAN ARMY

AUTHOR: Otávio Prochmann Loebens
ADVISOR(A): Renan Viana Rocha

Electronic warfare is a fundamental factor in military conflicts today. Controlling the electromagnetic spectrum provides significant advantages and increases the chances of success for those who possess it. The objective of this work is to analyze the use of the electromagnetic spectrum and the importance of possessing sovereignty in this domain, based on some electronic warfare equipment used by the Russian and American armies, and how they were used in some conflicts, such as the Gulf War, the Syrian War, and the Russo-Ukrainian War. Additionally, it seeks to highlight the lessons learned from these conflicts and how they affect the Brazilian Army. Through bibliographic and documentary research, Russian and American electronic warfare systems were demonstrated, as well as events involving these systems in current conflicts. The justification for this work is the need to understand how electronic warfare can strongly influence the outcomes of a conflict, highlighting the capabilities and limitations of the world's major powers in this field, in order to present results that can improvethe electronic warfare capabilities of the Brazilian Army. It was possible to conclude that Brazil needs to invest more resources in materials, doctrine, and personnel training to keep up with the constant technological advancements in electronic warfare.

Palavras-chave: Electronic warfare. Eletromagnetic spectrum. Brazilian Army. Conflicts.

LISTA DE FIGURAS

Figura 1 - Desfile de viaturas de GE chinesas 9
Figura 2 - Faixas do espectro eletromagnético 11
Figura 3 - Operações no espectro eletromagnético 12
Figura 4 - Ações das MAGE 14
Figura 5 - Ações das MAGE 16
Figura 6 - Ações das MAGE 17
Figura 7 - Vista a estibordo do AN/SLQ-32 18
Figura 8 - Instalação de um ALQ-99 TJS em uma aeronave 19
Figura 9 - AIDEWS pod – AN/ALQ-211 (V)8 19
Figura 10 - AN/MLQ-40 (V)3 Prophet 20
Figura 11 - AN/TPQ-53 equipado com antena IFF 21
Figura 12 - Sistema Borisoglebsk-2 a bordo de um blindado 22
Figura 13 - Sistema de GE Murmansk-BN3 22
Figura 14 - Sistema de GE Russo Krasukha-4 23
Figura 15 - Sistema de GE Russo Palantin 23
Figura 16 - Sistema de GE Russo R-330Zh Zhitel 24
Figura 17 - Khibiny Jamming Pod 25
Figura 18 - Sistema 1L267 Moskva-1 25
Figura 19 - Sistema Leer RB-441V e VANT Orlan-10 26
Figura 20 - Drone capturado pelo Exército Russo após ataque 28
Figura 21 - Radar 1L122-1E 29
Figura 22 - Principais sistemas de GE utilizados na Ucrânia 32
Figura 23 - Sistemas de GE russos destruídos ou capturados 34
Figura 24 - R-330Zh destruído por drone ucraniano 35
Figura 25 - Parte do sistema Krasukha-4 36

SUMÁRIO

1. INTRODUÇÃO 8
1.1. OBJETIVOS 9
1.1.1. Objetivo geral 9
1.1.2. Objetivos específicos 9
2. REFERENCIAL TEÓRICO 11
2.1. ESPECTRO ELETROMAGNÉTICO 11
2.2. GUERRA ELETRÔNICA 12
2.2.1. Medidas de Apoio de Guerra Eletrônica 14
2.2.2. Medidas de Ataque Eletrônico 15
2.2.3. Medidas de Proteção Eletrônica 16
2.3. PRINCIPAIS POTÊNCIAS EM GE NO MUNDO 17
2.3.1. Estados Unidos Da América 17
2.3.2. Rússia 21
2.4. A GE NOS CONFLITOS ATUAIS 26
2.4.1. Guerra do Golfo 26
2.4.2. Guerra da Síria 27
2.4.3. Guerra Russo-Ucraniana 30
3. REFERENCIAL METODOLÓGICO 37
3.1. TIPO DE PESQUISA 37
3.2. MÉTODOS 37
4. RESULTADOS E DISCUSSÕES 38
5. CONSIDERAÇÕES FINAIS 41
REFERÊNCIAS 43

1. INTRODUÇÃO

O mundo está em constante evolução e junto a isso, as guerras também estão. No passado as batalhas eram travadas utilizando apenas o espaço terrestre e com o passar do tempo, novos ambientes operacionais foram criados. Para garantir, ou ter mais chances de êxito em uma guerra, o domínio desses campos é essencial.

O domínio do espectro eletromagnético é fator decisivo no campo de batalha, pois é por ele que são utilizados, através da guerra eletrônica, diversos equipamentos essenciais para as operações nos diferentes ambientes operacionais. A guerra eletrônica é responsável por atuar no espectro eletromagnético buscando utilizar eficientemente as suas emissões eletromagnéticas próprias, ao mesmo tempo que visa impedir, atrapalhar ou extrair informações das emissões inimigas (BRASIL, 2019).

Segundo o manual C 34-1, Emprego da Guerra Eletrônica, o marco inicial da GE foi na Batalha Naval de Tsushima, quando pela primeira vez foram interceptadas comunicações de telegrafia sem fio (TSF), fato que foi decisivo para o término da batalha Russo-Japonesa.

A partir daí, visto a importância da interceptação, bloqueio ou monitoramento das atividades de comunicação do inimigo para a decisão de um conflito, o foco para a criação de novas tecnologias que se utilizam de meios eletromagnéticos, tanto para se proteger quando para atacar o inimigo, aumentou consideravelmente. Essa evolução fica clara ao analisar os conflitos que se desencadearam até os dias atuais.

Muito tempo após a Batalha Naval de Tsushima, na Guerra do Golfo, foi possível perceber que o emprego da GE foi responsável por multiplicar o poder de combate dos aliados, ajudando consideravelmente na diminuição de baixas (BRASIL, 2019). Atualmente, é possível notar a importância e a ampla utilização da GE como fator multiplicador do poder de combate na Guerra Russo-Ucraniana.

Assim é oportuno problematizar a questão: a GE brasileira está suficientemente preparada frente as maiores potências visto os exemplos da importância que a guerra eletrônica possui nos conflitos militares?

Há, ainda, outras questões de estudo que podem ser apontadas, pois é importante saber como o domínio do espectro eletromagnético pode influenciar no resultado de uma guerra, evidenciando quais as vantagens de se ter uma constante evolução na GE do país.

Com base nesses questionamentos, este trabalho busca analisar a importância do GE e

do domínio do espectro eletromagnético como elemento decisório e fator multiplicador do poder de combate.

Esta pesquisa se justifica, pois é imprescindível que o Exército Brasileiro esteja em constante evolução em seus diversos campos de atuação. Não é diferente com a Guerra Eletrônica, visto que grandes potências militares estão dando ênfase para esse ramo. A demonstração de força dos chineses, por exemplo, ao desfilarem com suas novas unidades de GE e o sucesso dos equipamentos russos na guerra com a Ucrânia evidenciam essa importância da preocupação com o constante aperfeiçoamento dos nossos métodos, doutrinas e equipamentos de GE. Portanto, é necessário analisar a utilização do espectro eletromagnético por outros países que participaram ou estão participando de conflitos militares para extrair ensinamentos que possam contribuir para as medidas de apoio de guerra eletrônica, medidas de ataque eletrônico e medidas de proteção eletrônica da GE do Exército Brasileiro.

Figura 1- Desfile de viaturas de GE chinesas

Fonte: autor desconhecido

1.1. OBJETIVOS

1.1.1. Objetivo geral

Evidenciar a importância da soberania do espaço eletromagnético a partir da análise de conflitos militares e identificar os reflexos para o Exército Brasileiro.

1.1.2. Objetivos específicos

Conceituar o espectro eletromagnético e apresentar os principais equipamentos militares utilizados nas diversas faixas do espectro eletromagnético;

Identificar a GE como fator multiplicador do poder de combate em conflitos militares tendo como base os equipamentos utilizados; e

Apresentar ensinamentos extraídos na utilização da GE nesses conflitos e identificar os reflexos para o Exército Brasileiro.

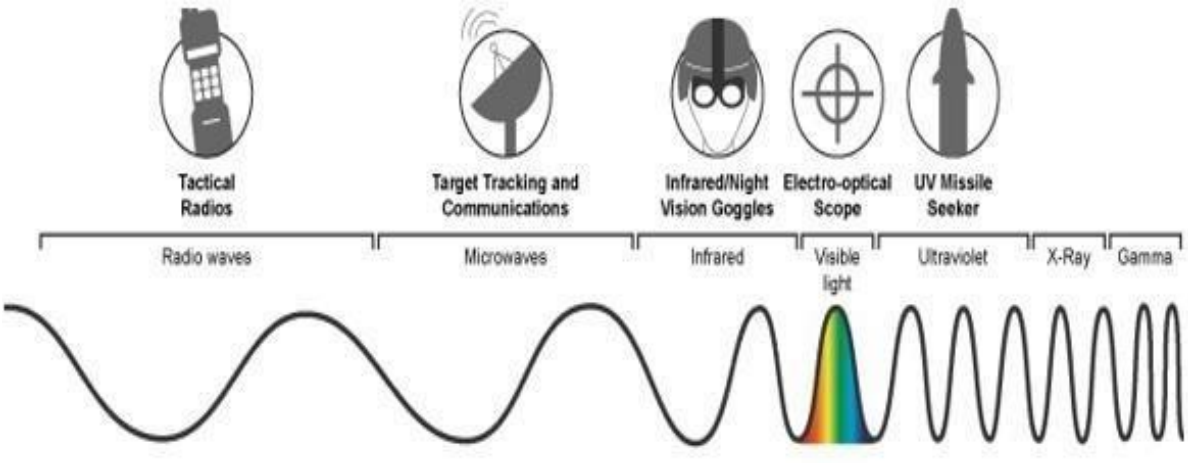
2. REFERENCIAL TEÓRICO

2.1. ESPECTRO ELETROMAGNÉTICO

O espectro eletromagnético (EMS) é composto por ondas eletromagnéticas com distintas frequências e comprimentos de onda. Esses, são fatores essenciais para determinar quais são as interações entre a matéria e as ondas eletromagnéticas (SALICIO, 2016). Assim, cada intervalo de frequências corresponde a uma faixa espectral e possuem diferentes características e interações com a matéria.

O EMS da suporte para diversas formas de utilização tanto civis quanto militares, desde redes para celulares até rádios e armamentos (GAO, 2021). Dentro do meio militar, cada faixa espectral possui equipamentos essenciais para o domínio de todos os campos, como por exemplo, equipamentos de visão noturna, rádio táticos, radares, entre outros.

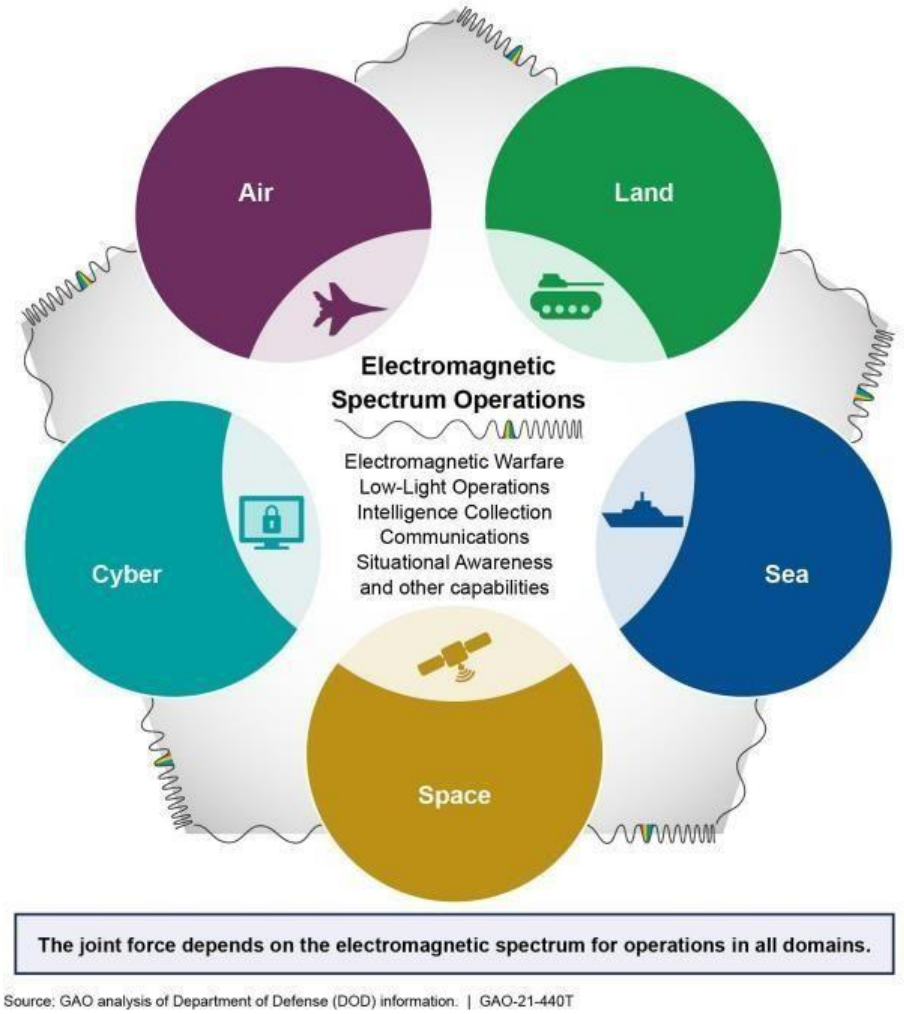
Figura 2 - Faixas do espectro eletromagnético



Fonte: GAO, 2021.

É importante destacar que nos combates atuais o domínio do EMS é fator essencial para alcançar a superioridade nos diversos ambientes operacionais, afetando diretamente operações terrestres, aéreas, marítimas, espaciais e cibernéticas (DoD, 2020).

Figura 3 - Operações no espectro eletromagnético



Fonte: GAO, 2021.

2.2. GUERRA ELETRÔNICA

Segundo o manual EB70-MC-10.223, Operações, a GE é composta por atividades que têm como objetivo assegurar o emprego de emissões eletromagnéticas com eficiência e proporcionar liberdade de uso do espectro eletromagnético para forças amigas e, simultaneamente, atrapalhar as emissões inimigas, além de explorar e negar a liberdade da utilização do espectro pelos mesmos.

De acordo com o manual FM 3-12 do Exército dos EUA *Cyberspace and electronic warfare operations*, a guerra eletrônica é conceituada por ações militares que fazem a utilização de enrgia eletromagnética e direta para controlar o espectro eletromagnético ou atacar o inimigo.

> A guerra eletrônica é uma consequência direta da evolução da tecnologia de detecção e comunicações ocorrida durante e depois da Segunda Grande Guerra Mundial. A invenção dos radares, aperfeiçoamento dos sistemas de interceptação e interferência de ondas de rádio e da criptografia, revolucionou a forma como se fazia a guerra até então. Agora aviões poderiam ser detectados bem antes de chegar a seus alvos,

> ordens de comandantes poderiam ser enviadas as suas tropas a distâncias muito maiores do que jamais tinha sido feito, ou, serem interceptadas favorecendo forças inimigas (NETO, 2017).

A GE atua em dois campos diferentes: o de comunicações e o de não comunicações. O primeiro é responsável por utilizar equipamentos para o trânsito de informações, já o segundo utiliza os sinais e equipamentos na produção de informações (BRASIL, 2019).

Ainda segundo o Manual C 34-1, a GE também se divide em 03 (três) diferentes ramos. As Medidas de Apoio de Guerra Eletrônica (MAGE) são responsáveis por obter informações do inimigo, de forma passiva, a partir da análise das emissões eletromagnéticas de interesse utilizada por ele. As Medidas de Ataque Eletrôncio (MAE) por meio de técnicas de reflexão, irradiação, absorção de energia eletromagnética e outros, procuram atrapalhar ou até impedir o uso do espectro eletromagnético pelo inimgo. Já as Medidas de Proteção Eletrônica (MPE) são responsáveis por proteger as próprias emissões eletromagnéticas, visando a atuação da GE inimiga ou também interferências não intencionais.

As MAGE se dividem em diferentes tipos de ações, sendo elas a Busca e interceptação (BI), Monitoração (Mon), Localização Eletrônica (Loc Elt), Registro (REG) e Análise de GE (Anl Ge). Todas as ações tem o objetivo final de coletar dados e informações, buscando obter vantagem sobre o inimigo.

As MAE podem ser Destrutivas e Não-destrutivas, sendo a primeira dividida em ações de Emissão de Energia Direcionada (EED) e Guiamento de Armas pela Emissão do Alvo (GAEA) e buscam causar dano físico ao inimigo. A segunda é dividida em Bloqueio (Blq) e Despistamento (Dptt) e tem como objetivo apenas impedir que o inimigo utilize o espectro eletromagnético com eficácia, sem causar qualquer dano fisico à ele.

As MPE se dividem em ações antiMAGE e antiMAE, que visam negar ao inimigo a utilização de MAE e MAGE sobre as tropas amigas.

A alta utilização das diferentes faixas do espectro eletromagnético, seja por emissores civis como militares, impõe que a GE tenha em mente suas prioridades na busca por informações do inimigo. Deve ser atribuida a missões que compensem seu emprego e tenham objetivos muito bem definidos, além de decisivos e atingíveis (BRASIL, 2019).

Ademais, para que a GE posso ser decisiva como multiplicadora do poder de combate, as MAE, MAGE e MPE devem estar em sintonia com a missão recebida e com os objetivos a serem atingidos, além de estarem perfeitamente integrados (BRASIL, 2019)

2.2.1. Medidas de Apoio de Guerra Eletrônica

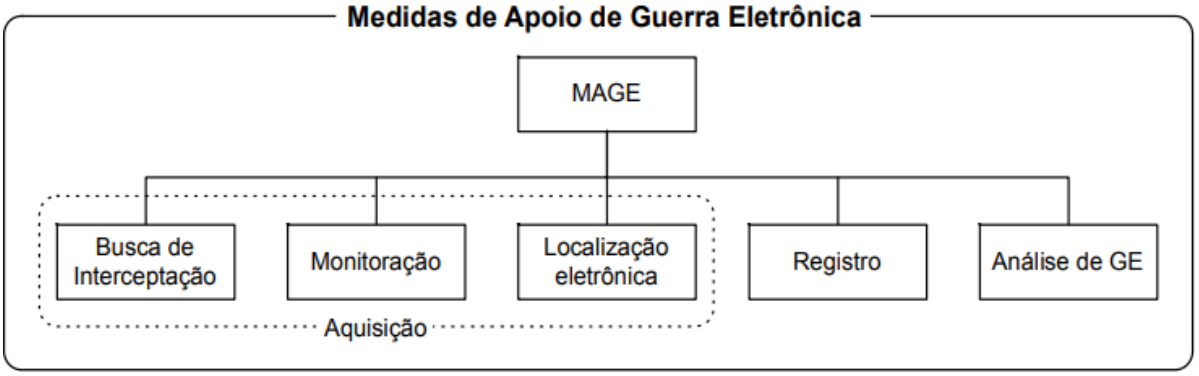
Esse ramo da GE é responsável pela obtenção e análise de dados capturadas a partir de emissões eletromagnéticas inimigas, dessa forma capturam dados e parâmetros suficientes para determinar o tipo de ameaça, seu modo de operação e sua provável localização (BRASIL, 2019).

No campo de comunicações, as MAGE atuam identificando e localizando emissores de comunicações do inimigo, já no campo de não comunicações localizam emissores de não comunicações e sistemas de armas associados, dessa forma atuam dando suporte para o planejamento e execução das Medidas de Ataque Eletrônico (BRASIL, 2019).

As MAGE são a base da GE e uma das fontes de informação mais importantes na tomada de decisão em todos os níveis de comando, pois possuem uma rápida e oportuna reação às ameaças ao permitirem as ações das MAE e das MPE, além disso tem a capacidade de avaliar os sistemas eletrônicos inimigos e amigos a partir da análise a avaliação de dados coletados pela Inteligência do Sinal (BRASIL, 2019).

As ações de MAGE são divididas em 05 (cinco) ramos, sendo eles a Busca e Interceptação, Monitoração e Localização Eletrônica, que fazem parte da Aquisição, e o Registro e Análise de GE.

Figura 4 - Ações das MAGE



Fonte: Manual EB70-MC-10.201, 2019.

A Busca e Interceptação é a ação que tem por objetivo interceptar e reconhecer sinais ativos de interesse, com a finalidade de identificá-los e classificá-los, determinando também, a direção de sua chegada. Os sistemas modernos das MAGE tem a capacidade de fazer a busca e interceptação automática de sinais (BRASIL, 2019).

A monitoração é a ação que visa observar e acompanhar uma emissão eletromagnética de interesse cujo o objetivo é de acompanhar as atividades e a evolução dessa emissão, além de obter outros dados relevantes. Sistemas modernos das MAGE realizam essa ação juntamente com a Busca e Interceptação (BRASIL, 2019).

A Localização Eletrônica é a ação que consiste em determinar, por meio de sistemas especializados, a provável posição de um emissor de energia eletromagnética. Para isso, os equipamentos devem formar algum arranjo geométrico específico e estar a uma distância suficiente entre si. A precisão da localização depende de vários fatores, sendo alguns deles as condições climáticas e ambientais do momento, a configuração topográfica do terreno, a posição dos postos das MAGE e o adestramento de pessoal (BRASIL, 2019).

O Registro consiste no armazenamento dos sinais de interesse com o objetivo de analisar posteriormente seus metadados e parâmetros técnicos (BRASIL, 2019).

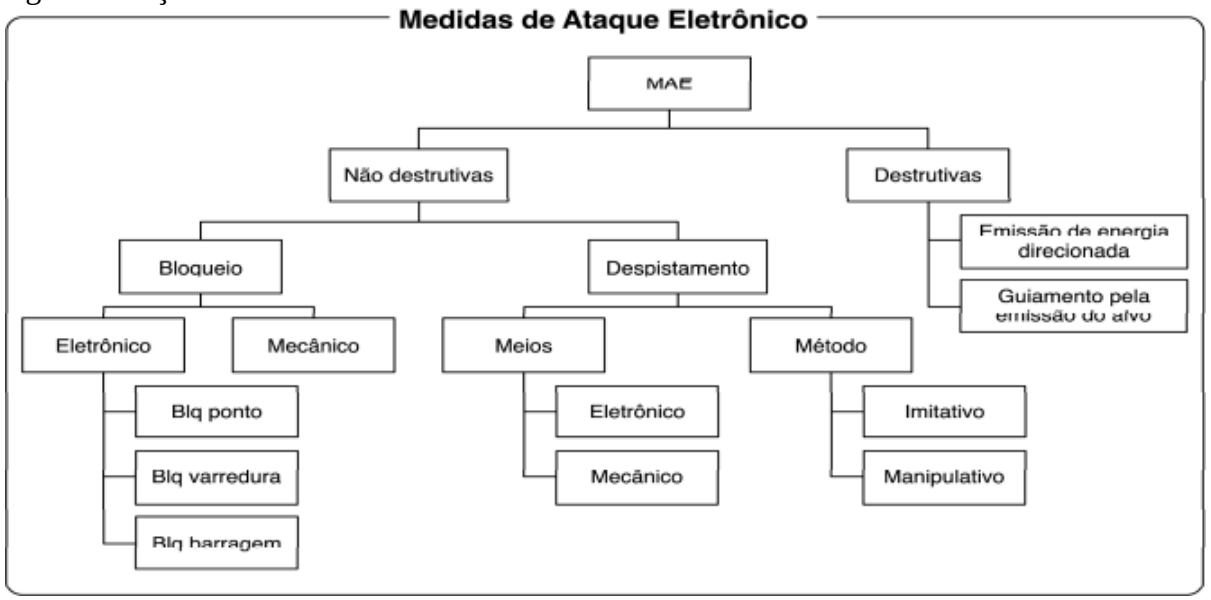
A Análise de Guerra Eletrônica é a ação que consiste em investigar, correlacionar e interpretar todos os resultados e informações obtidas das emissões eletromagnéticas interceptadas com o objetivo de produzir conhecimentos e novas informações. É dividido em análise de conteúdo, análise de tráfego, análise de localização eletrônica, análise técnica e análise final. Além disso possuem uma classificação quanto ao tempo, sendo divididas em análise imediata, análise corrente e análise de longo prazo (BRASIL, 2019).

2.2.2. Medidas de Ataque Eletrônica

As MAE englobam atividades que objetivam enfraquecer a capacidade de combate do adversário, através do impedimento da utilização eficaz do espectro eletromagnético pelo inimigo, induzindo-lhe ao erro. Essas ações podem ser realizadas por meio de radiações, reirradiações, reflexões, alterações, ou absorções intencionais de energia eletromagnética, ou também, pela destruição física dos sistemas eletrônicos oponentes através de energia direcionda de alta potência (BRASIL, 2019).

As MAE são divididas em ações não destrutivas e destrutivas, sendo a primeira, ainda, separada em técnicas de bloqueio e técnicas de despistamento.

Figura 5 - Ações das MAGE



Fonte: Manual EB70-MC-10.201, 2019.

As ações não destrutivas consistem em empregar a emissão, retransmissão, absorção ou reflexão de energia eletromagnética com o objetivo de degradar ou impedir os sistemas eletrônicos inimigos sem lhes causar dano físico direto (BRASIL, 2019).

A técnica de bloqueio tem como finalidade degradar e negar a utilização do espectro eletromagnético pelo inimigo por meio de técnicas ativas e passivas, respectivamente obloqueio eletrônico e o bloqueio mecânico (BRASIL, 2019).

A técnica do despistamento consiste na utilização do espectro eletromagnético de forma que induza o oponente ao erro na interpretação e uso das informações recebidas pelos seus sistemas eletrônicos (BRASIL, 2019).

As ações destrutivas consistem em ações que utilizam o espectro eletromagnético para causar dano físico ao inimigo e aos seus sistemas eletrônicos. São classificadas em ações de emissão de energia direcionada e guiamento de armas pela emissão do alvo, sendo que, a primeira consiste na emissão direcionada de radiação de alta potência capaz de infligir dano ao material e pessoal inimigo, e o segundo, consiste na utilização de armamentos com sensores próprios que são guiados pela emisão eletromagnética de sistemas inimigos. (BRASIL, 2019).

2.2.3. Medidas de Proteção Eletrônica

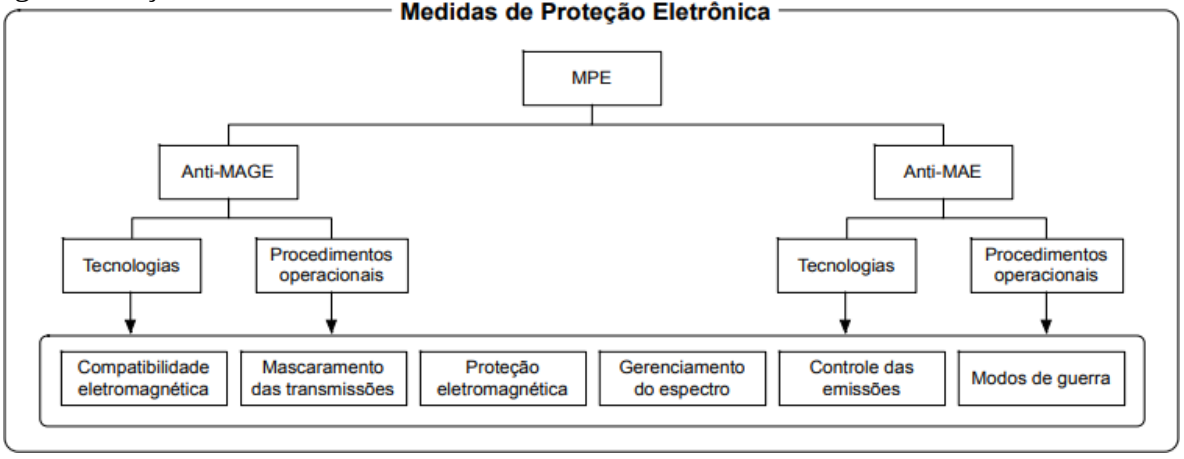
As MPE são ações defensivas que consistem em assegurar a utilização do espectro eletromagnético pelas forças amigas. Elas tem o objetivo de proteger tanto pessoal quanto material amigo da utilização do espectro magnético EM ações que visem degradar, destruir ou

inviabilizar as capacidades de combate amigas (BRASIL, 2019).

Quando empregadas corretamente, as MPE diminuem significativamente as chances de sucesso do inimigo nas ações de MAE e MAGE próprias, inviabilizando a exploração e o ataque oponente (BRASIL, 2019).

As MPE são divididas em ações anti-MAGE e anti-MAE.

Figura 6 - Ações das MAGE



Fonte: Manual EB70-MC-10.201, 2019.

As ações anti-MAGE tem como objetivo impedir que o oponente seja eficaz em suas ações de interceptação, monitoração, localização eletrônica, registro e análise de emissões amigas (BRASIL, 2019).

As ações anti-MAE tem como objetivo reduzir ou neutralizar os efeitos das MAE utilizadas pelo adversário, bem como minimizar os danos indesejados causados pelas MAE utilizadas pelas forças amigas (BRASIL, 2019).

2.3. PRINCIPAIS POTÊNCIAS EM GE NO MUNDO

2.3.1. Estados Unidos da América

O país é um dos mais avançados no quesito tecnologia militar no geral, principalmente na GE, devido a altos investimentos destinados ao ramo. Possui uma grande e poderosa quantidade de equipamentos, sendo algum deles: AN/SLQ-32, AN/ALQ-99, AN/ALQ-211, AN/MLQ-40 e AN/TPQ-53.

O AN/SLQ-32 é o principal sistema de GE que é integrado aos navios da Marinha americana. O sistema foi colocado em operação nos anos 80 e vem recebendo diversas atualizações para melhorar a sua eficiência em um projeto chamado SEWIP (*Surface Electronic*

Warfare Improvemente Program) que promete extender o tempo de vida do equipamento.

O AN/SLQ-32 é um sistema de guerra eletrônica responsável pela detecção de mísseis antinavio utilizando processamento assistido para identificação automática e instantânea de sinais interceptados. Seu principal objetivo é aumentar a defesa do navio contra mísseis de cruzeiro antinavio e outras armas de características de frequências de rádio similares. Seu objetivo secundário é detectar e identificar emissões eletromagnéticas dentro da área operacional do navio (SCHULER, 1994).

Figura 7 - Vista a estibordo do AN/SLQ-32

Fonte: The U.S. National Archives, 2000.

Segundo a Navair, O AN/ALQ-99 é um sistema tático de *jamming* para aeronaves com capacidade de ataque eletrônico. O sistema é carregado na parte externa da aeronave e pode ser utilizado para suprimir radares e as comunicações inimigas. Além disso, o sistema passou por diversas atualizações para manter sua capacidade diante das novas ameaças emergentes.

Figura 8 - Instalação de um ALQ-99 TJS em uma aeronave

Fonte: Defense Visual Information Distribution Service, 2011.

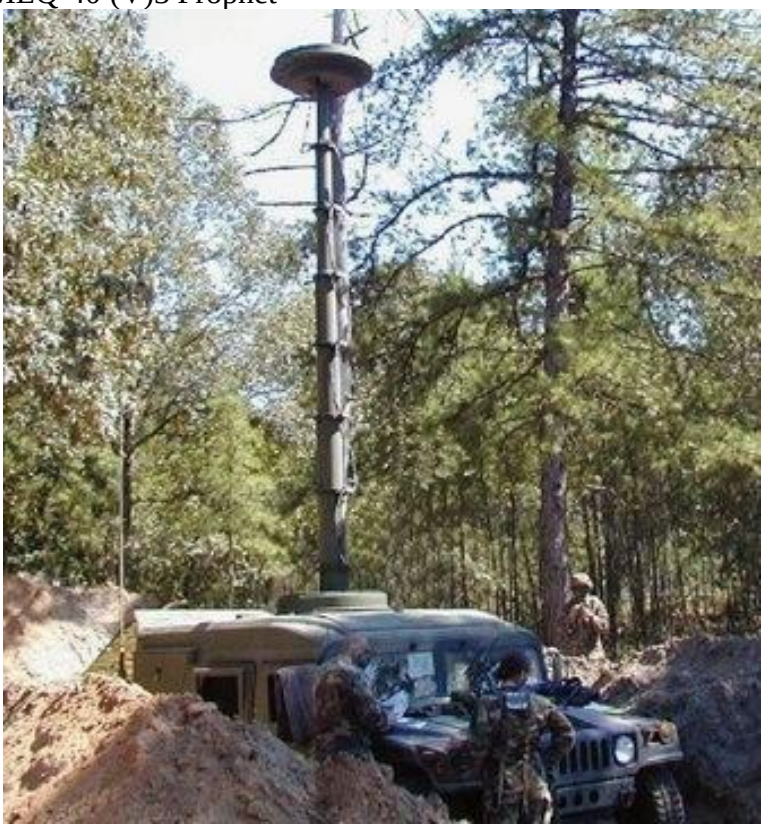
De acordo com a empresa L3HARRIS, desenvolvedora do equipamento, o ALQ-211 é uma família de sistemas que detectam, negam, degradam, interrompem e evitam ameaças letais, além de fornecer consciência situacional em diversos espectros, sejam frequências rádio, infravermelho ou laser. Quando a aeronave equipada com esse quipamento entra em uma situação ameaçadora, o ALQ-211 estabelece a distância da ameaça em relação a aeronave e caso esteja em alcance letal o sistema inicia uma resposta de contramedidas de frequência de rádio instantânea, bloquando a ameaça.

Figura 9 - AIDEWS pod – AN/ALQ-211 (V)8

Fonte: Sydney Freedberg, 20

O sistema AN/MLQ-40 Prophet é um sistema de inteligência do sinal e guerra eletrônica que tem a capacidade de mapear emissores de rádio frequência de 20MHz até 2000MHz, além de poder realizar ataques eletrônicos interceptando comunicações por voz e bloqueando as transmissões inimigas (MASSON, 2006).

Figura 10 - AN/MLQ-40 (V)3 Prophet



Fonte: Deagel, 2007.

O AN/TPQ-53, de acordo com a empresa Lockheed Martin, é um sistema de radar terrestre, com boa mobilidade, confiabilidade e suportabilidade, que tem a capacidade de detectar, classificar, rastrear e determinar a posição do ataque inimigo, além de ter a habilidade de identificar e rastrear drones, possibilitando que um único equipamento realize monitoramento e contra aquisição de alvos.

Figura 11 - AN/TPQ-53 equipado com antena IFF

Fonte: Lockheed Martin, 2021.

2.3.2. Rússia

A Rússia está entre as maiores potências mundiais militares em todas as áreas bélicas, inclusive na Guerra Eletrônica. Nesse ramo, possui sistemas com capacidade de bloquear armas inimigas e sistemas eletrônicos, além de proteger instalações militares e órgãos governamentais amigos de ameaças externas. Desde 2009, a Rússia vem modernizando seus sistemas de GE (DA COSTA, 2022).

Alguns dos principais equipamentos de GE utilizados pelos russos incluem o Krasukha-4, Murmansk-BN, Palantin, Borisoglebsk-2, R-330Zh Zhitel, Khibiny, Moskva-1 e o Leer-3 RB-341V.

O sistema de GE Borisoglebsk-2 é um complexo de interferência multifuncional de inteligência de sinais que foi projetado para obstruir transmissões de informações via satélite, sistemas de navegação por rádio e de comunicação terrestre e aérea nas frequências HF, VHF e UHF (ODIN, s.d.). Além disso, o sistema é capaz de rastrear, identificar e interromper em sinais de frequência fixa e de salto de frequência. Com isso, tem a capacidade de bloquear frequências utilizadas por drones e minas terrestres remotamente controladas, impedindo o controle do adversário sobre esses dispositivos.

Figura 12 - Sistema Borisoglebsk-2 a bordo de um blindado

Fonte: Ministério de Defesa da Federação Russa, 2019.

Conforme dito por Army Recognition (2022), o Murmansk-BN é um dos sistemas de GE maiseficientes do mundo. O sistema é capaz de conduzir reconhecimentos de rádio, interceptar e suprimir sinais adversários nas faixas de 3 a 30 MHz e atuar, principalmente, nas comunicaçõesmilitares de HF da Organização do Tratado do Atlântico Norte (OTAN) e dos EUA. O principalalvo desse equipamento é o High Frequency Global Communications System (HFGCS) que é o sistema de comunicações HF utilizado pela Força Aérea americana.

Figura 13 - Sistema de GE Murmansk-BN

Fonte: Thomas Withington, 2021.

Segundo Odin ([s.d.]), o sistema Krasukha-4 é um módulo móvel de GE fabricado pela própria Rússia. Foi projetado para neutralizar satélites espiões de baixa altitude, radares,

sistemas aéreos de alerta e controle (AWACS) e sistemas de orientação de armamentos por radar em raios entre 150 e 300 quilômetros. Além disso, o equipamento tem a capacidade de criar uma poderosa inteferência em frequências essenciais para radares e outras fontes emissoras de frequências rádio, podendo causar dano aos equipaments de GE inimigos.

Figura 14 - Sistema de GE Russo Krasukha-4

Fonte: Ministério da Defesa da Federação Russa, 2021

De acordo com o Ministério de Defesa da Federação Russa, o sistema Palantin é capaz de derrubar veículos aéreos não tripulados de reconhecimento e interferir em pontos de acesso de celular e fontes de internet sem prejuízo para a infraestrutura civil, pois atua pontualmente. O equipamento tem alcance de mais de 20 quilômetros e pode ainda, detectar e neutralizar automaticamente linhas de comunicação por rádio, inclusive digitais.

Figura 15 - Sistema de GE Russo Palantin

Fonte: Samuel Cranny-Evans, 2019

Segundo Army Recognition, o sistema R-330Zh Zhitel é responsável por detectar, localizar e interferir em estações móveis de comunicação via satélite Inmarsat e Iridium, estações-base de celular GSM 1900 e equipamentos de navegação que utilizam o sistema de satélites NAVSTAR (GPS).

Figura 16 - Sistema de GE Russo R-330Zh Zhitel

Fonte: Denis Abramov, 2018

O sistema Khibiny, de acordo com o Ministério de Defesa da Federação Russa, é um complexo de GE aéreo construído para detectar e inteferir em sinais de rádio emitidos pelo inimigo, distorcendo as informações que são refletidas. Além disso, tem a capacidade de detectar aeronaves de GE inimigas, camuflar alvos de interesse entre sinais falsos e mensurar distância, velocidade e posição angular de um objeto. O equipamento é fixado nas asas de uma aeronave, ficando suspenso sendo capaz de analisar o espectro eletromagnético e decidir quando utilizar, ou não, uma interferência de acordo com um algoritimo especial.

Figura 17 - Khibiny Jamming Pod

Fonte: Ministério da Defesa da Federação Russa, 2021

O Moskva-1, segundo o site Army Recognition, é um radar complexo e moderno que tem a capacidade de detectar e rastrear alvos aéreos em até 400 quilômetros, além de conseguir classificar os emissores em níveis de ameaça. Esse sistema consegue operar em um sistema passivo, ou seja, pode receber e analisar sinais externos sem que emita qualquer tipo de sinal, permanecendo invisível ao inimigo.

Figura 18 - Sistema 1L267 Moskva-1

Fonte: Vitaly V. Kuzmin, 2015

O sistema Leer-3 RB-341V, de acordo com o Ministério de Defesa da Federação Russa, foi projetado para suprimir o sistema global para comunicações móveis (GSM), utilizando

interferência de rádio instalada em um VANT, veículo aéreo não tripulado. Os Orlan-10 são os VANTS responsáveis por esses ataques. São equipados com transmissores que simulam a rede GSM, impedindo a utilização de terminais pessoais. Além disso o sistema pode ser utilizado no envio de mensagens falsas.

Figura 19 - Sistema Leer RB-341V e VANT Orlan-10

Fonte: Topwar, 2015

2.4. A GE NOS CONFLITOS ATUAIS

2.4.1. Guerra do Golfo

A guerra do golfo teve início em 1990 após a invasão do Kuwait pelo exército iraquiano. Tal ação provocou uma grande preocupação na comunidade internacional, principalmente nos EUA, visto que o Iraque passou a ter o controle de cerca de 20% das reservas mundiais de petróleo e passava a configurar uma ameaça para à Arábia Saudita.

Por isso, após o insucesso da retirada das tropas iraquianas do Kuwait pela ordem da Organização das Nações Unidas, os EUA lideraram um coalizão para expulsar o Iraque do Kuwait, fato alcançado após a Operação Desert Storm em fevereiro de 1991 (SILVA, [s.d.]).

Na guerra do golfo, tanto o Iraque quanto os EUA buscavam obter novos e modernos equipamentos de GE, através de grandes esforços em pesquisas de novas tecnologias, pois a GE foi essencial para o sucesso das forças da coalizão (MORALES apud MOSSI, 2019).

Os EUA utilizaram as MAGE a fim de varrer o espectro eletromagnético, coletando e analisando emissões para levantar informações utilizando aeronaves de combate de GE, submarinos realizando operações de reconhecimento e vigilância e utilização de satélites na

produção de informações de não comunicações (MORALES apud MOSSI, 2019).

Além disso os americanos se utilizavam de mensagens falsas em transmissões para confundir os iraquianos. Através de suas MAGE, o Iraque, buscava informações no espectro e, conseguiam, por exemplo, notar uma diminuição do tráfego nas comunicações dos americanos antes de um ataque aéreo e conseguiam avisar a tempo as baterias antiaéreas amigas (MORALES apud MOSSI, 2019).

Os iraquianos utilizavam-se de meios físicos para obterem uma transmissão de informações mais segura, se utilizando de fibras ópticas e linhas telefônicas enterradas. Porém, .após esses meios físicos serem alvos de operações dos americanos, os iraquianos foram forçados a utilizarem ligações rádio, o que comprometia o alto comando iraquiano, já que grande parte das informações eram interceptadas pelos americanos (MORALES apud MOSSI, 2019).

Nas MAE, os americanos utilizaram suas aeronaves que, quase em sua totalidade, possuíam sistemas e emissores externos ou internos capazes de interferir nas comunicações inimigas (MORALES apud MOSSI, 2019).

Além disso, outra MAE que foi de fundamental importância e ampla utilização, foi a utilização dos chaffs, sistema responsável pela liberação de pedaços de alumínio, plástico ou fibras de vidro com o objetivo de desviar mísseis direcionados a uma aeronave (MOSSI, 2019).

2.4.2. Guerra da Síria

A guerra civil na Síria teve seu início com protestos pacíficos contra o ditador Bashar Al-Assad, porém foram reprimidos com violência pelo governo. A partir daí os protestos passaram a ser armados pelos rebeldes que se opunham ao governo sírio. Esse conflito atraiu grupos terroristas como a Al-Qaeda e o Estado Islâmico para a região, que se aproveitaram da situação para expandir suas influências. Mas, eles não foram os únicos, outros países decidiram intervir no conflito de acordo com seus interesses próprios.

Quatro grupos principais são responsáveis pelos conflitos na Síria, sendo eles: o governo sírio, apoiado principalmente pela Rússia; os rebeldes e curdos; a Al-Qaeda e o Estado Islâmico; e os Estados Unidos e seus aliados.

A partir daí, todos iniciaram conflitos pelos seus interesses, sendo que os Russos apoiavam o governo Sírio (com interesse em manter o seu monopólio sobre o gás natural para a Europa), enquanto os EUA e aliados buscavam derrubar o governo sírio para manter sua hegemonia militar e combater os extremistas islâmicos (MOSSI, 2019).

Disso, inicia-se um conflito entre russos e americanos, pois eram eles os fornecedores

dos equipamentos para os distintos lados do conflito.

O campo de batalha Sírio se tornou um grande campo de testes para os armamentos e equipamentos russos, entre eles os seus equipamentos de guerra eletrônica.

As capacidades Russas de GE foram muito bem exploradas na Síria, pois ao receberem em suas bases um ataque de enxames de drones dos sírios, demonstraram possuir um efetivo sitemas frente a esse tipo de ameaça. Em janeiro de 2018, 13 drones carregados com explosivos foram direcionados às forças russas. De acordo com o Ministério de Defesa da Rússia, os seus sistemas de GE foram capazes de neutralizar seis desses drones, tomando seuscontroles e os pousando em locais específicos. Tal fato demonstrou a efetividade do *spoofing* de GPS da Rússia, que pode emitir um sinal até 500 vezes mais forte que os sinais originais (EGOZI, 2019).

Figura 20 - Drone capturado pelo Exército Russo após ataque

Fonte: Ministério da Defesa da Federação Russa, 2019

A Rússia criou um sistema que integra defesa aérea e guerra eletrônica chamado A2D2 (*anti-access/area denial*). Consiste na utilização de sistemas de lançamento de mísseis e equipamentos de guerra eletrônica para se obter o controle do espaço aéreo sírio.

Esses meios de GE integrados ao sistema, multiplicaram a eficiência da defesa do espaço aéreo na região, já que bloqueiam as comunicações e os sistemas de navegação de aeronaves que invadirem território proibido para voo (MOSSI, 2019).

Os russos utilizaram diversos sistemas de GE na Síria com o objetivo de obter a superioridade no domínio do espectro eletromagnético e, consequentemente, do espaço aéreo sírio. Sistemas como a série de radares 1L122 e os sistemas móveis de GE como o Krasukha-

4, Leer-3, Zoopark-1 e Moskva-1, foram utilizados para atingir esse objetivo.

O radar 1L122-1E pode detectar uma diversidade de alvos como helicópteros, aeronaves, mísseis de cruzeiro e veículos aéreos não tripulados (VANTS).

Figura 21 - Radar 1L122-1E

Fonte: Standfair Operations, 2019

O sistema Krasukha-4 evitou um ataque a uma base aérea russa localizada na Síria ao tornar ineficaz ataques de mísseis controlados por rádio, devido a interferência causada pelo equipamento (MOSSI, 2019).

O sistema Leer-3 RB-341V foi utilizado para enviar mensagens para facções rebeldes com solicitações de armstício (PECK, 2017).

Tanto a Rússia quanto os EUA estavam ativos na Síria, local onde já foi possível notar a força da guerra eletrônica russa, visto que o campo de batalha sírio foi descrito como o ambiente de guerra eletrônica mais agressivo do planeta e os russos mantinham certa superioridade. Ao operarem próximos e contra os russos, os americanos foram testados constantemente, pois tinham seus sistemas de comunicações derrubados diversas vezes (SMITH, 2020).

De acordo com Vladimir Neelov, as armas de guerra eletrônica russas são superiores aos sistemas americanos em diversos parâmetros, principalmente no quesito alcance. Para ele, essa superioridade se dá, particularmente, pela efetividade dos sistemas contra VANTs demonstrada na Síria (VARFOLOMEEVA, 2018).

Além disso, o conflito na Síria serviu de ensinamento para o exército russo, que pôde identificar e compreender limitações de seus equipamentos de GE e levantar oportunidades de melhoria para que, mais a frente, pudessem ser implementadas modernizações em seus sistemas de forma a ampliar suas capacidades nesse ramo.

2.4.3. Guerra Russo-Ucraniana

A guerra entre a Rússia e a Ucrânia se desencadeou devido a diversas razões, entre elas a expansão da OTAN pelo Leste Europeu e a possível adesão da Ucrânia a essa Aliança Militar. Esse fato enfureceu o presidente russo, Vladimir Putin, que optou por invadir a Ucrânia com a justificativa de que estava impedindo um suposto cerco à sua fronteira pela OTAN, além de proteger os ucranianos de origem russa que vivem em Donetsk e Luhansk e tem o desejo de se tornarem parte da Rússia.

A Rússia possui unidades especializadas em guerra eletrônica para conduzir suas operações de MAE e MAGE. Suas forças terrestres são compostas por brigadas de guerra eletrônica atreladas a 05 (cinco) distritos militares russos para dar apoio as operações regionais de GE. Essas brigadas são equipadas com os sistemas Krasukha-2 e Krasukha-4, Leer-3, Moskva-1 e Murmansk-BN. Além disso, cada brigada de manobra do exército russo possui uma companhia de GE responsável por atuar dentro dos 50 quilômetros de distância, utilizando-se de sistemas menores como o Zhitel (CLARK, 2022).

Alguns especialistas apontaram a Rússia como uma força que possui algumas das unidades mais experientes e bem equipadas do mundo, por isso, no início da invasão, os analistas já esperavam que os russos dominassem o espectro eletromagnético rapidamente (CLARK, 2022).

Os esforços russos foram, em grande parte, despendidos com guerra eletrônica no conflito com a Ucrânia, visto que pelo menos três das cinco brigadas de GE russas estão voltadas para esse conflito e, ainda, possuem uma grande capacidade contra equipamentos da OTAN, que estão sendo usados pelos ucranianos, pois os operadores de guerra eletrônica russos já possuem experiência após enfrentar esses mesmos esquipamentos na Guerra da Síria (CLARK, 2022).

Os esforços ucranianos estão sendo no sentido de evoluir sua GE para alcançar a Rússia,

que demonstrou uma superioridade no controle do espectro eletromagnético. Ambos os países herdaram seus equipamentos da antiga União Soviética, por isso possuem sistemas semelheantes, mas os russos tiveram uma evolução muito maior nesse ramo, principalmente, devido a participação na guerra civil Síria, onde puderam corrigir as falhas e modernizar seus equipamentos.

Dessa forma, os sistemas ucranianos encontram várias dificuldades contra os russos. Um dos exemplos é o drone Orlan-10, drone russo que possui capacidade de voar em altitudes superiores ao alcance máximo dos equipamentos ucranianos de GE, conforme dito pelo coronel Ucraniano Dmytro Kashchenko (ANTONIUK, 2022).

A utilização pela comunicação por satélites se mostrou essencial para os Ucranianos no conflito contra os russos. As tropas ucranianas estão utilizando amplamente o acesso ao serviço de internet Starlink (sistema da empresa de foguetes privada de Elon Musk), pois é possível acessar o serviço com pequenas antenas parabólicas de fácil utilização, permitindo que os ucranianos continuem se comunicando mesmo com redes de internet e celular totalmente bloquadas pelos russos (MARQUARDT, 2022).

Os russos, ao perceberem a utilização do Starlink pelos Ucranianos, logo começaram a desenvolver técnicas para derrubar esse sistema, porém, segundo Elon Musk, foram lançadas novas atualizações de segurança para conter a ofensiva russa. Entretanto, os russos encontraram maneiras de degradar a comunicação desse sistema e localizar seus usuários, o que é possível notar a partir de declarações de soldados que lutam a favor dos ucranianos sobre serem rápidos ao utilizarem esse tipo de equipamento para não serem pegos pelos russos. (SKOVE, 2023)

Na guerra entre Rússia e Ucrânia os equipamentos utilizados pelos russos são praticamente os mesmos utilizados na Guerra da Síria, porém com a bagagem de já terem sido utilizadas anteriormente.

Figura 22 - Principais sistemas de GE utilizados na Ucrânia

Electronic Warfare System	Purpose	First Fielded	Notes
1RL257 Krasukha-4	Targets X-band and K $_u$-band radars, particularly on planes, drones, missiles, and low-orbit satellites	2014	Consists of two KamAZ-6350 trucks, one a command post and the other outfitted with sensors
1L269 Krasukha-2	Targets S-band radars, particularly on airborne platforms. Often used paired with the Krasukha-4	2011	Also based on two KamAZ-6350 trucks
RB-341V Leer-3	Disrupts VHF and UHF communications, including cellular communications and military radios, over hundreds of kilometers	2015	Consists of a truck-based command post that works with Orlan-10 drones to extend its range
RH-330Zh Zhitel	Jammer; can shut down GPS and satellite communications over a radius of tens of kilometers	2011	Consists of a truck command post and four telescopic-mast phased-array antennas
Murmansk-BN	Long-range detection and jamming of HF military radios	2020	Russian sources claim it can jam communications thousands of kilometers away
R-934B	VHF/UHF jammer that targets wireless and wired communications	1996	Consists of either a truck or a tracked vehicle and a towed 16-kilowatt generator
SPN-2, 3, 4	X- or K $_u$-band jammers that target airborne radars and air-to-surface guidance-control radars	(not available)	Consists of a combat-control vehicle and an antenna vehicle
Repellent-1	Antidrone system	2016	Weighs more than 20 tonnes
Moéskva-1	Precision HF/VHF receiver for passive coherent location of enemy ships and planes	2015	Published sources cite a range of up to 400 kilometers

Fonte: Bryan Clark, 202

Um dos sistemas amplamente utilizado pelos russos contra os ucranianos foi o Leer RB-341V, como afirma Withington:

> Um notório sistema de GE implantado pelo exército russo foi o RB-341V Leer-3, que usa veículos aéreos não tripulados (UAVs) para bloquear redes celulares. Ele desempenhou um papel importante no bloqueio de telefones celulares usados por tropas e civis ucranianos. O RB-341V foi pensado para ser usado para enviar mensagens de texto falsas e desmoralizantes para as tropas ucranianas e para rastrear seus movimentos. Esta última informação foi traduzida em alvos para a artilharia russa (WITHINGTON, 2022).

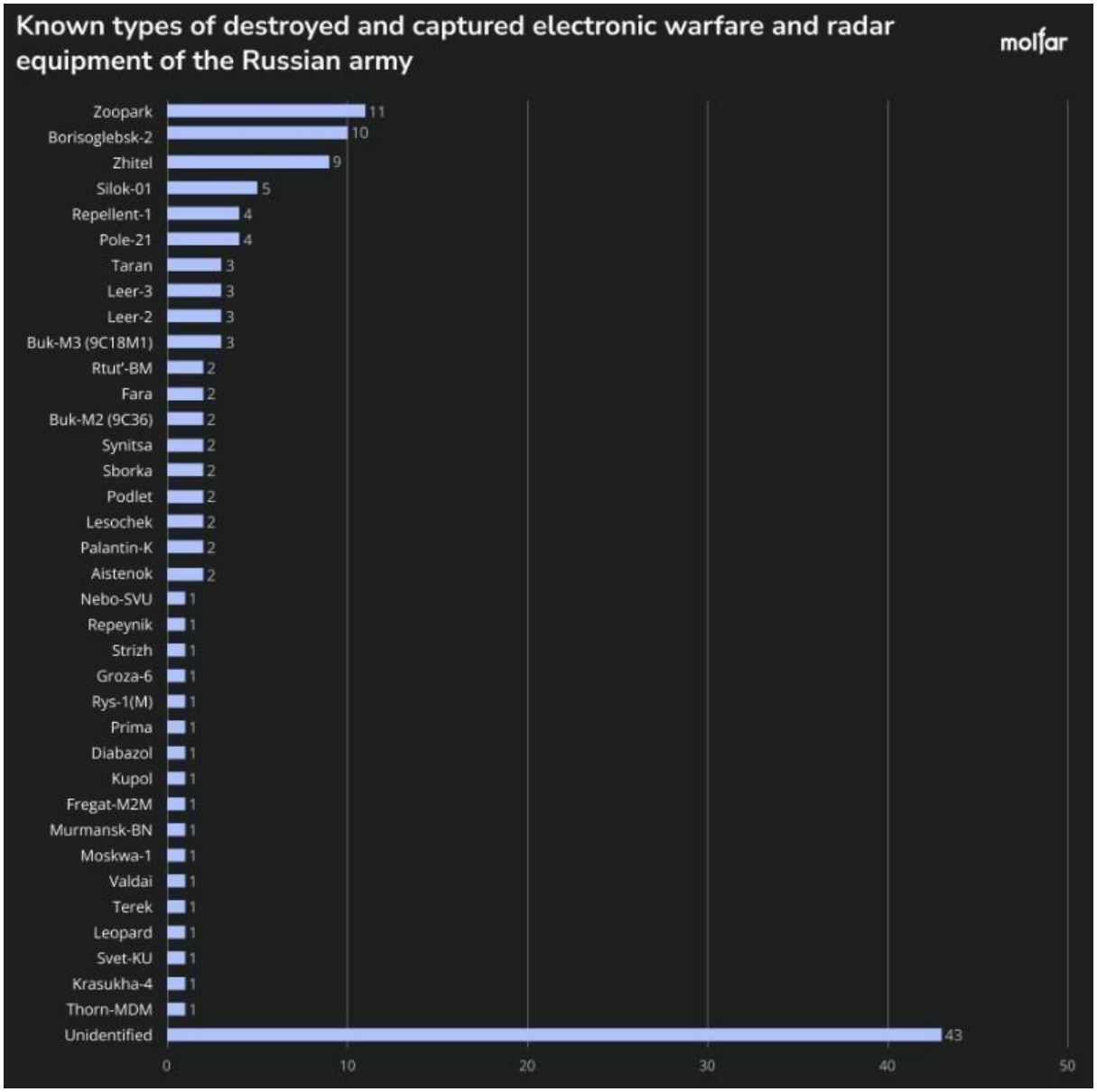
Durante o conflito com a Ucrânia, foi possível identificar inúmeras ações de guerra eletrônica no campo de batalha, principalmente contra VANTs, com o objetivo de negar inteligência ao inimigo, o que é essencial visto que a utilização desses sistemas aéreos não tripulados são de vital importâcia nos conflitos atuais. Além disso, mesmo durante as ações na Ucrânia, a Rússia foi capaz de implementar melhorias ou até novas tecnologias em seus equipamentos de Guerra Eletrônica (DA COSTA, 2022).

Um dos exemplos desse contínuo aprimoramento dos sistemas de GE russo, foi a intensificação dos bloqueios realizados ao sistema de lançamento de mísseis mais temido e respeitado utilizado pelos ucranianos, o HIMARS, diminuindo fortemente sua eficácia (BERTRAND, 2023).

É importante destacar, também, que os sistemas de GE são alvos extremamente valiosos em um conflito, porque tanto a destruição quanto apossamento desses sitemas são de vital importância para os resultados.

De acordo com a agência Molfar OSINT, no campo de batalha ucraniano foram identificadas 133 destruições, danos ou capturas de sistemas de guerra eletrônica russa, causando um prejuizo de cerca de 1 bilhão de dólares. Entre os sistemas mais atacados estão: Zoopark, Borisoglebsk e Zhitel.

Figura 23 - Sistemas de GE russos destruídos ou capturados



Fonte: Molfar Osint, 2023

Ainda segundo essa agência, cerca de 82% desses sistemas russos foram destruídos, 4,5% foram danificados e 13,5% foram capturados.

Figura 24 - R-330Zh destruído por drone ucraniano

Fonte: Autor desconhecido, 2023

Um exemplo de equipamento capturado foi o Krasukha-4. O exército ucraniano conseguiu ter posse desse avançado sistema, fato importante para a inteligência inimiga dos ucranianos, que pôde ter acesso a um dos melhores e mais completos sistemas russos de GE.

> Um curioso 'contêiner' que as tropas ucranianas capturaram hoje parece representar uma perda russa significativa e uma potencial mina de ouro de inteligência. O que as forças da Ucrânia encontraram parece ser um posto de comando em contêiner que faz parte do sistema de guerra eletrônica móvel Krasukha-4. O Krasukha-4 foi projetado principalmente para detectar e bloquear grandes radares, como os de alerta antecipado e aeronaves de controle, como o E-3 Sentry da Força Aérea dos EUA e satélites espiões. (TREVITHICK, 2022)

Figura 25 - Parte do sistema Krasukha-4

Fonte: Autor desconhecido, 2023

Ao analisar todos esses acontecimentos é possível perceber uma preocupação da OTAN em relação às capacidades russas de guerra eletrônica, sejam na capacidade de bloquear radares, suas defesas antiaéreas e até bloquear sistemas de internet em grandes porções da região europeia (DA COSTA, 2022).

A preocupação com as capacidades russas também levou aos ucranianos utilizarem meios físicos para a comunicação, como por exemplo um telefone por manivela, que foi utilizado na primeira guerra mundial, pois dessa forma não podem ser detectados nem interceptados pelos avançados sistemas russo de guerra eletrônica. Segundo soldados ucranianos, o telefone a manivela é o sistema mais seguro para se comunicar e apesar de ser um equipamento antigo, funciona muito bem (BEALE, 2023).

3. REFERENCIAL METODOLÓGICO

Os procedimentos metodológicos utilizados foram leituras preliminares de manuais e artigos para aprofundamento do tema;

3.1. TIPO DE PESQUISA

Este trabalho apresentou característica bibliográfica, visto que todo referencial teórico foi analisado para chegar ao resultado final da pesquisa, de forma que, com base nos equipamentos utilizados pelas principais potências em GE mundiais, a guerra eletrônicapudesse ser interpretada como fator multiplicador do poder de combate e relacionada com as guerras do Golfo, Síria e Russo-Ucraniana, destacando sua importância nesses conflitos. Para isso, foram utilizados como suporte a pesquisa bibliográfica em diversos artigos, revistas e reportagens, entre eles “A comparação entre o emprego da guerra eletrônica (GE) nas guerras de terceira e quarta geração: a GE na guerra do Golfo e na guerra civil Síria” (MOSSI, 2019), e pesquisas documentais em manuais, entre eles o Manual C- 34-1 Emprego da Guerra Eletrônica (BRASIL, 2019).

3.2. MÉTODOS

A pesquisa em bancos de dados eletrônicos se deu utilizando-se como palavras-chave: guerra eletrônica – espectro eletromagnético – electronic warfare – guerra russo-ucraniana – guerra da síria – guerra do golfo. O material utilizado, baseado nas pesquisas documentais e bibliográficas, compõe o referencial teórico e foi devidamente referenciado. Os resultados e discussões presentes no trabalho tiveram como base os referencias teóricos.

4. RESULTADOS E DISCUSSÕES

O campo de batalha que um dia foi linear e previsível, hoje, agrega uma diversidade de atores e diferentes ambientes operacionais, o que demanda que os comandantes, em todos os escalões, possuam uma ampla flexibilidade de planejamento e emprego de meios que, com o passar dos anos, são cada vez mais complexos. Por esse motivo, vários novos fatores tornaram-se essenciais na influência do desobramento de sistemas militares (BRASIL, 2019).

Existe uma alta demanda por uma constante e precisa consciência situacional, sendo essencial nos processos de tomadas de decisões: o planejamento e execução de ações; a importância na sincronização e coordenação de manobras suportados por um sistema de comando e controle eficiente; e o grande avanço tecnológico em diversas áreas, proporcionando limites de atuaçãomais profundos, manobras mais precisas. Esses são alguns dos fatores que tornaram a utilização do espectro eletromagnético essencial nos ambientes operacionais, incrementando a utilizaçãode sistemas de tecnologia ds informação e comunicações (BRASIL, 2019).

Com a maior utilização do espectro eletromagnético, novos sistemas e fontes foram criadas, porém junto a elas, novas vulnerabilidades surgiram, pois a emissão de energia eletromagnética pode ser interceptada e explorada. Quando empregada em consoância com o coneceito de uma operação, a GE se mostra um importante fator multiplicador do poder de combate, sendo indispensável no planejamento e condução de uma operação (BRASIL, 2019).

O espectro eletromagnético, nos conflitos atuais, é amplamente utilizado por diversos equipamentos com diferentes frequências e cada um com sua funcionalidade, responsáveis por alterar os rumos de um combate, seja atuando nas MAE, MAGE ou MPE. Por esse motivo, é evidente a necessidade em se obter o domínio desse campo de atuação, pois é um fator essencial para a multiplicação do poder de combate de uma força.

A busca pela superioridade militar no mundo é uma corrida sem fim e é perceptível a preocupação das maiores potências mundiais, entre elas os EUA, a Rússia e a China, em possuir um maior controle sobre o espaço eletromagnético e demonstrar suas capacidades nesse ramo. Os EUA já possuem modernos sistemas de guerra eletrônica que foram colocados em uso em situações reais, demonstrando suas capacidades e limitações. Desde a guerra do Golfo até os dias atuais, foi possível notar uma grande modernização dos sistemas de GE americanos, que buscaram ampliar suas capacidades nesse ramo, visto que foi de grande importância para o sucesso no conflito.

O exército americano possui uma diversidade de equipamentos, sejam em

plataformas terrestres, aéreas ou marítimas, esse fato contribui para que o país seja uma das maiores potências mundias militares. Mesmo assim, com a guerra Russo-Ucraniana e os perceptíveis avanços tecnológicos da GE chinesa, os americanos se mostram preocupados e necessitados em maiores investimentos nesse ramo. Tal fato é perceptível na fala do diretor de informações do Pentágono, Jhon Sherman, que afirmou que a medida que os EUA se preparam para a China, devem ser capazes de lutar e dominar o espectro eletromagnético, e ainda concluiu dizendo que a dinâmica da utilização desse espectro, tanto pelos russos quanto pelos ucranianos, deve ser acompanhada (SPUTNIK, 2023).

A Rússia, por sua vez, é o país mais temido no quesito domínio do espectro eletromagnético. Já demonstrou uma grande força nesse aspecto na Guerra da Síria, onde utilizou seus equipamentos de forma eficiente, provendo inteligência e consciência situacional a sua tropa ao mesmo tempo que negava a utilização do espectro pelo inimigo. Na Síria, os modernos sistemas russos já possuiam numerosas capacidades, mas também possuíam limitações. Com a guerra, foi possível identificar essas limitações para que futuramente esses sistemas fossem melhorados e pudessem ser empregados de forma mais eficiente, tal fato aconteceu e está acontecendo na guerra Russo-Ucraniana.

Outro importante fator nos conflitos atuais e que a Rússia possui um efetivo sistema para neutralização, é a utilização dos Veículos Aéreos Não Tripulados, os VANTs, que estão surgindo cada vez mais como protagonistas.

A guerra Russo-Ucraniana está demonstrando a força do Exército Russo no domínio do espectro eletromagnético. Tal fato, não só desenvolve o Exército Russo, como também liga a luz de alerta de vários outros países que percebem que estão ficando para trás na corrida pela superioridade no espectro eletromagnético. Assim como na Guerra Fria, que houve a corrida armamentista, como uma concorrência sobre quem possuía a maior superioridade bélica com maior poder de destruição, hoje, existe essa mesma corrida armamentista para definir quem possui maior superioridade sobre o controle do espectro eletromagnético.

Através da análise na guerra do Golfo, na guerra da Síria e, mais atualmente, no conflito entre a Rússia e a Ucrânia, é possível observar a importância da Guerra Eletrônica e como se tornou essencial possuir o domínio do espectro eletromagnético, que constitui um fator decisivo na condução de operações militares.Fica evidente que uma força militar possuidora do controle desse campo de atuação terá seu poder de combate multiplicado frente às demais forças.

Em relação ao Brasil, é importante destacar que o país tem se mostrado preocupado com o aumento da relevância da Guerra Eletrônica nas últimas décadas e vem buscando se preparar

para lidar com essa ameaça. Simultaneamente à constante evolução dos combates modernos, tanto na parte doutrinária, quanto na parte tecnológica, a GE do Exército Brasileiro tem se atualizado, adaptando-se a todas essas evoluções (BRASIL, 2019).

É interessante que o Brasil aprenda com as experiências vividas por outros países em conflitos reais, para que dessa forma possa continuar se atualizando e buscando as melhores soluções de adestramento e equipamentos de Guerra Eletrônica. Nesse sentido, o Exército Brasileiro deve se empenhar em buscar esses tipos de ensinamentos, identificando os reflexos para a sua própria atuação, e buscando aprimorar de maneira contínua sua doutrina de GE.

O investimento do Brasil em Guerra Eletrônica ainda é, no entanto, considerado baixo, se colocado em comparação com outros países, dos quais destacam-se os EUA, Rússia e China, potências mundiais nesta área. Além disso, ainda persistem várias limitações, dentre as quais podem ser citadas a falta de investimento em tecnologias nacionais, a falta de pessoal capacitado e a falta de equipamentos adequados.

Torna-se necessário ao país que as forças armadas, com o auxílio da indústria de defesa, desenvolvam e aprimorem suas capacidades de guerra eletrônica, buscando o desenvolvimento nacional de meios de GE, para diminuir essa dependência externa, além de permanecer em condições de acompanhar a rápida evolução tecnológica desses equipamentos.

O enfrentamento desses desafios demanda que o Exército Brasileiro mantenha um adestramento que não se limite ao uso de tecnologias vulneráveis à efeitos da Guerra Eletrônica. Atividades como a orientação, por exemplo, devem ser realizadas de modo a não depender de dispositivos eletrônicos, como o GPS. Ou seja, habilidades como a orientação carta-terreno e azimute-distância devem continuar sendo estimuladas, apesar da facilidade ofertada pelo geoposicionamento.

De forma semelhante, não é interessante que os comandantes de frações estejam excessivamente dependentes de tecnologias de comunicações e comando e controle para executar suas missões. É importante que o comando tenha clareza no planejamento e em suas ordens, já que em um conflito, esses meios tecnológicos podem ser inviabilizados por ataques eletrônicos inimigos.

Apesar do avanço observado nas últimas décadas na doutrina, capacitação e nos equipamentos empregados no Brasil, nota-se que ainda há muito a ser feito em relação a Guerra Eletrônica para que o Exército Brasileiro alcance o mesmo patamar dos exércitos das potências militares mundiais.

5. CONSIDERAÇÕES FINAIS

A Guerra Eletrônica é uma área que tem se mostrado cada vez mais importante nos conflitos militares modernos. Com o avanço da tecnologia, a capacidade de controlar o espectro eletromagnético tornou-se um fator decisivo na condução de operações militares. As potências mundiais têm investido pesadamente em tecnologias que ampliem suas capacidades de GE.

Essas tecnologias possibilitam à força militar detentora um controle maior sobre o campo de batalha, podendo interferir nas comunicações inimigas, desativar sistemas eletrônicos e obter informações valiosas sobre as forças adversárias. Além disso, a GE pode ser utilizada para proteger as próprias forças militares contra ataques eletrônicos inimigos.

Com base nas análises desenvolvidas neste trabalho, pode-se concluir que a Guerra Eletrônica é um fator multiplicador do poder de combate e possui grande importância nos conflitos militares modernos. Através da revisão bibliográfica e análise dos equipamentos utilizados pelas principais potências mundiais em GE, foi possível identificar algumas das principais tecnologias e táticas utilizadas nesse tipo de guerra.

Os objetivos da pesquisa foram alcançados ao identificar a importância da Guerra Eletrônica nos conflitos atuais e seus reflexos para o Exército Brasileiro. Foi possível constatar que as potências mundiais possuem amplas capacidades em GE, como demonstrado nos conflitos descritos no trabalho, sobretudo nas guerras do Golfo, da Síria e na mais recente disputa entre Rússia e Ucrânia.

No entanto, apesar da importância da Guerra Eletrônica nos conflitos atuais, o Brasil ainda possui sérias limitações nessa área. Embora tenha apresentado alguma evolução em doutrina, material e capacitação de pessoal, o país ainda precisa investir mais recursos para estar melhor preparado aos desafios da Guerra Eletrônica moderna.

Nesse sentido, sugere-se a realização de novos trabalhos que avaliem a evolução da Guerra Eletrônica nas doutrinas das potências mundiais e como o Brasil pode acompanhar esse processo. Sugere-se ainda estudos sobre como o Brasil poderia ampliar seu investimento em capacitação de pessoal, aquisição de material e adequação da doutrina. Isso incluiria, por exemplo, a necessidade de treinamentos específicos para as tropas, aquisição de novos equipamentos e a atualização constante das doutrinas militares.

Sugerem-se ainda que sejam realizados estudos para identificar com mais precisão as atuais limitações do país nesta área, por exemplo, meios de comunicações utilizados pelas forças armadas que possam apresentar vulnerabilidades de GE, buscando também soluções para superá-las, além de avaliar a necessidade do desenvolvimento de tecnologias de GE nacionais,

com o objetivo de diminuir a dependência externa e falta de autonomia nessa área, o que também poderia impactar positivamente a soberania nacional.

Por fim, é fundamental que o Exército Brasileiro esteja atento às tendências e evoluções da Guerra Eletrônica, além de continuar investindo em equipamentos e adestramento de militares. A capacidade de ampliar o poder de combate através do uso dessas tecnologias avançadas pode constituir um fator decisivo em futuros conflitos.

REFERÊNCIAS

1RL257 KRASUKHA-4. **Army Recognition**, 2022. Disponível em: https://www.armyrecognition.com/russia_russian_military_field_equipment/krasukha-4_1rl257_broadband_multifunctional_jamming_station_electronic_warfare_system_technical_data_sheet_pictures_video_10610156.html#pictures. Acesso em: 24 jul. 2022

1RL257E Krasukha-4 Russian 8x8 Mobile Multifunctional Jammer. **ODIN**, [s.d.]. Disponível em: https://odin.tradoc.army.mil/WEG/Asset/f039dd3d04fa0226088d1257319579a7. Acesso em: 24 jul. 2022.

ALQ-99 Tactical Jamming System. **Navair**, [s,d]. Disponível em: https://www.navair.navy.mil/product/ALQ-99-Tactical-Jamming-System. Acesso em: 25 abr. 2023.

AN/ALQ-211 CV-22, NH 90, and F-16 Self Protection System. **L3harris**, [s.d]. Diponível em: https://www.l3harris.com/all-capabilities/alq-211-cv-22-nh-90-and-f-16-self-protection-system. Acesso em: 25 abr. 2023.

AN/TPQ-53 Radar System. **Lockheed Martin**, [s.d]. Disponível em: https://www.lockheedmartin.com/en-us/products/tpq-53.html. Acesso em: 25 abr. 2023.

ANTONIUK, Daryna. How electronic warfare is reshaping the war between Russia and Ukraine. **The Record**, 2022. Disponível em: https://therecord.media/how-electronic-warfare-is-reshaping-the-war-between-russia-and-ukraine. Acesso em: 05 mai. 23.

BEALE, Jonathan. A tecnologia da Primeira Guerra Mundial que está ajudando a Ucrânia a enganar a Rússia. **BBC**, 2023. Disponível em: https://www.bbc.com/portuguese/articles/c168zd53616o. Acesso em: 09 mai. 2023.

BRASIL C 34-1: **Emprego da Guerra Eletrônica**, 2. ed. Brasília, DF: EME, 2019.

CLARK, Bryan. The Fall and Rise of Russian Electronic Warfare. **IEEE Spectrum**, 2022. Disponível em: https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare. Acesso em: 25 abr. 2023.

DA COSTA, Vinicíus Machado. **A Guerra Eletrônica Russa nos conflitos atuais**. Rio de Janeiro: EsACosAAe, 2022. Disponível em: http://www.esacosaae.eb.mil.br/images/phocagallery/2022/pdf/radareguerraeletronica/Artigo_de_Opinio_-_1_Ten_Vinicius_Costa_-_GE_russa.pdf. Acesso em: 09 mai. 2023.

Destruction of electronic warfare equipment as a prelude to a counteroffensive. Analytics confirms dates of counteroffensive announced by the Ministry of Defense of Ukraine. **Molfar**, 2023. Disponível em: https://www.molfar.global/en-blog/electronic-warfare-equipment-of-russian-occupiers. Acesso em: 09 mai. 2023.

DA COSTA, Vinicíus Machado. **A Guerra Eletrônica Russa nos conflitos atuais**. Rio de Janeiro: EsACosAAe, 2022. Disponível em: http://www.esacosaae.eb.mil.br/images/phocagallery/2022/pdf/radareguerraeletronica/Artigo_de_Opinio_-_1_Ten_Vinicius_Costa_-_GE_russa.pdf. Acesso em: 09 mai. 2023.

Destruction of electronic warfare equipment as a prelude to a counteroffensive. Analytics confirms dates of counteroffensive announced by the Ministry of Defense of Ukraine. **Molfar**, 2023. Disponível em: https://www.molfar.global/en-blog/electronic-warfare-equipment-of-russian-occupiers. Acesso em: 09 mai. 2023.

EGOZI, Arie. Why Would Russia Spoof Israeli GPS? F-35 & Iran. **Breaking Defense**, 2019. Disponível em: https://breakingdefense.com/2019/06/if-russia-is-spoofing-israeli-gps-then-why-iran-f-35/?fbclid=IwAR3UIVjaJT72jH7zQqqmit9KFeLS%202ixDmZkrN6COARXTpP87OnrmTbm4smg. Acesso em: 25 abr. 2023.

EUA. Exército dos EUA. **The U.S. Army Operating Concept**, 2014.

EW and Leer-3 crews continue tasks in special military operation. **Ministry of Defence of the Russian Federation**, 2022. Disponível em: https://eng.mil.ru/en/news_page/country/more.htm?id=12442096@egNews. Acesso em: 29 abr. 2023.

HENKE, Philip T**. Lessons Learned and Forgotten: Electronic Warfare in the United States Army**. US Army School for Advanced Military Studies, 2021.

MARQUARDT, Alex; BERTRAND, Natasha; COHEN, Zachary. Russia's jamming of US-provided rocket systems complicates Ukraine's war effort. **CNN**, 2023. Disponível em: https://edition.cnn.com/2023/05/05/politics/russia-jamming-himars-rockets-ukraine/index.html. Acesso em: 09 mai. 2023.

MARQUARDT, Alex; LYNGAAS, Sean. Ucrânia tem interrupção na comunicação por falta de financiamento de satélites da Starlink. **CNN**, 2022. Disponível em: https://www.cnnbrasil.com.br/internacional/ucrania-tem-interrupcao-na-comunicacao-por-falta-de-financiamento-de-satelites-da-starlink/. Acesso em: 09 mai. 2023.

MASSON, Scott R. **Unmanned Aerial Vehicle Use in Army Brigade Combat Teams: Increasing Effectiveness Across the Spectrum of Conflict**. NAVAL POSTGRADUATE SCHOOL MONTEREY CA, 2006.

MOSSI, Welder Passos. **Comparação entre o emprego da guerra eletrônica (GE) nas guerras de terceira e quarta geração: a GE na guerra do Golfo e na guerra civil Síria**. 2019.

Murmansk-BN. **Army Recognition**, 2022. Disponível em: https://www.armyrecognition.com/russia_russian_military_field_equipment/murmansk-bn_electronic_warfare_communications_jamming_system_data.html. Acesso em: 29 abr. 2023.

PECK, Michael. THE CRAZY WAY RUSSIA COULD HIJACK YOUR IPHONE. 2017. **The National Interest**, 2017.Disponível em: https://nationalinterest.org/blog/the-buzz/the-crazy-way-russia-could-hijack-your-iphone-19976. Acesso em: 24 jul. 2022.

Pentágono: EUA têm de reavivar e dominar novamente a guerra eletrônica. **Sputnik Brasil**, 2023. Disponível em: https://sputniknewsbrasil.com.br/20230310/pentagono-eua-tem-de-reavivar-e-dominar-novamente-a-guerra-eletronica-28006410.html. Acesso em: 25 abr. 2023.

RB, Gama Neto. **Guerra cibernética/Guerra eletrônica: conceitos, desafios e espaços de interação**. Política Hoje, v. 26, n. 1, p. 201-17, 2017.

Russia could deliver electronic warfare systems Moskva-1 and Rtut-BM to Iran 11511151. **Army Recognition**, 2015. Disponível em: https://www.armyrecognition.com/november_2015_global_defense_security_news_uk/russia_could_deliver_electronic_warfare_systems_moskva-1_and_rtut-bm_to_iran_11511151.html. Acesso em: 29 abr. 2023.

Russian Armed Forces electronic warfare professionals continue their combat tasks within special military operation. **Ministry of Defence of the Russian Federation**, 2022. Disponível em: https://eng.mil.ru/en/news_page/country/more.htm?id=12424260@egNews. Acesso em: 29 abr. 2023.

SCHULER, John W. **AN/SLQ-32 Operator Training: Development of Performance Assessment Instrument**. NAVY PERSONNEL RESEARCH AND DEVELOPMENT CENTER SAN DIEGO CA, 1994.

SILVA, Daniel Neves. Guerra do Golfo. **Mundo Educação**, [s.d.]. Disponível em: https://mundoeducacao.uol.com.br/historiageral/guerra-golfo.htm. Acesso em: 10 mai. 2023.

SKOVE, Sam. Using Starlink Paints a Target on Ukrainian Troops. **Defense One**, 2023. Disponível em: https://www.defenseone.com/threats/2023/03/using-starlink-paints-target-ukrainian-troops/384361/. Acesso em: 09 mai. 2023.

SMITH, Patrick. **Russian Electronic Warfare: A Growing Threat to US Battlefield Supremacy**. 2020.

SUEMONARO, Matti; CAFARELLA, Jennifer. Russia expands its air defense network in Syria. 2018. **ISW**, 2018. Disponível em: https://www.iswresearch.org/2018/11/russia-expands-its-air-defense-network.html. Acesso em: 24 jul. 2022.

TREVITHICK, Joseph. Ukraine just captured part of one of Russia's most capable electronic warfare systems. **The Drive**, 2022. Disponível em: https://www.thedrive.com/the-war-zone/44879/ukraine-just-captured-part-of-one-of-russias-most-capable-electronic-warfare-systems. Acesso em: 24 jul. 2022.

Ukrainian military hit the Russian R-330Zh Zhitel EW system. **Militarnyi**, 2023. Disponível em: https://mil.in.ua/en/news/ukrainian-military-hit-the-russian-r-330zh-zhitel-ew-system/. Acesso em: 09 mai. 2023.

US Navy receives AN/SLQ-32 Electronic Warfare system from Northrop Grumman. **Navy Recognition**, 2021. Disponível em: https://navyrecognition.com/index.php/naval-news/naval-news-archive/2021/june/10297-us-navy-receives-an-slq-32-electronic-warfare-system-from-northrop-grumman.html. Acesso em: 25 abr. 2023.

VARFOLOMEEVA, Anna. Signaling strength: Russia's real Syria success is electronic warfare against the US. **TheDefensPost**, 2018. Disponível em: https://www.thedefensepost.com/2018/05/01/russia-syria-electronic-warfare/. Acesso em 25 abr. 2023.

WITHINGTON, Thomas. Russia's electronic warfare capabilities have had mixes results agaist Ukraine. **The Drive**, 2022. Disponível em: https://www.thedrive.com/the-war-zone/this-is-whats-happened-so-far-in-ukraines-electronic-warfare-battle. Acesso em: 24 jul.2022.