0000-0000

DATA & HERTZ

Revista Científica de Guerra Eletrônica e Guerra Cibernética
do Centro de Instrução de Guerra Eletrônica

Volume 3 - jan./dez. 2023

ISSN 0000-0000

DATA & HERTZ

Revista Científica de Guerra Eletrônica e Guerra Cibernética
do Centro de Instrução de Guerra Eletrônica

Volume 3 - 2023

SUMÁRIO

Centro de Instrução de Guerra Eletrônica (CIGE)

Comandante
Ten Cel Com Joselito Rodrigues da Silva

Subcomandante
Ten Cel Com Luciano da Silva

Divisão de Ensino
Ten Cel Com Ezequiel da Silva Bastos

Seção de Guerra Eletrônica
Maj Com Bruno Elias Ribeiro

Seção de Guerra Cibernética
Maj Com Rodrigo Rocha Nunes

Seção de Doutrina
Maj Com Daniel Seixas da Silva

Seção de Pós-graduação
1º Ten OTT/Biblio Thaís Ribeiro Moraes Marques

Seção Biblioteca
1º Ten OTT/Biblio Thaís Ribeiro Moraes Marques

DATA&HERTZ – Revista Científica de Guerra Eletrônica e Guerra Cibernética do Centro de Instrução de Guerra Eletrônica / Centro de Instrução de Guerra Eletrônica.
Ano III, v. 3, n. 1, jan./dez. 2023 - Brasília-DF

Publicação Anual editada pelo Centro de Instrução de Guerra Eletrônica
ISSN 0000-0000

1. Centro de Instrução de Guerra Eletrônica 2. Defesa 3. Cibernética 4. Ciência & Tecnologia 5. Doutrina 6. Educação 7. Informática 8. Instrução Militar 9. Gestão 10. Operações Militares Conjuntas e Singulares.

CDD 350

Data & Hertz
Revista Científica de
Guerra Eletrônica e Guerra Cibernética
do Centro de Instrução de Guerra Eletrônica

A Revista Científica, Data & Hertz, editada e publicada pela Centro de Instrução de Guerra Eletrônica, tem por objetivo estimular e divulgar a produção científica no ramo das Ciências Militares, nas áreas relacionadas à Defesa, contribuindo efetivamente para o seu desenvolvimento.

OBJETIVOS

O periódico do Centro de Instrução de Guerra Eletrônica (CIGE) apresenta, sob a esfera científica, assuntos que englobam a Guerra Eletrônica e a Guerra Cibernética áreas do conhecimento de interesse do Exército Brasileiro, conforme as diretrizes do Conselho Editorial.

Tem, ainda, como missão, contribuir para o aperfeiçoamento dos recursos humanos, fornecendo subsídios necessários ao aprimoramento da cultura geral e profissional dos oficiais e graduados, estimular a participação de oficiais e praças nas atividades culturais, permitindo a divulgação das ideias e das experiências adquiridas durante a vida militar e contribuir para o desenvolvimento e o estudo da Doutrina Militar Terrestre.

O periódico busca democratizar a informação junto ao público interno sobre assuntos de interesse comum ao Exército e aos seus integrantes e divulgar junto ao público externo as atividades da Instituição reforçando a sua imagem perante a sociedade brasileira estimulando o autoaperfeiçoamento e o moral dos integrantes das Forças Armadas.

PÚBLICO-ALVO

O periódico tem como principais usuários: pesquisadores, professores, estudantes, profissionais das forças armadas, bem como, todos profissionais que atuam nas áreas de Defesa, Guerra Eletrônica, Cibernética, Ciência & Tecnologia, Direito Militar, Doutrina, Educação, Telecomunicações, Informática, Instrução Militar, Gestão, Operações Militares Conjuntas e Singulares, entre outras áreas correlatas.

PUBLICAÇÃO DE ARTIGOS

Os artigos apresentados para submissão devem ser livres de embaraços. Caso o autor tenha submetido o Artigo à outra revista, ele deverá consultar a mesma a respeito da submissão do artigo a esta Revista Científica, cientificando-se de não ferir direitos de publicação conferidos à revista anterior.

PROCESSO DE AVALIAÇÃO

Os artigos submetidos são avaliados pela Conselho Editorial no que se refere ao seu mérito científico e adequação às regras de apresentação de trabalhos científicos.

Em seguida, os textos são encaminhados aos pareceristas, tendo estes o prazo de 30 dias para fazerem a sua avaliação. Os pareceristas não são remunerados e, caso aceitem, terão seus nomes incluídos no Comitê de Avaliadores, publicados a cada volume da revista.

A partir das avaliações dos pareceristas, o Comitê Editorial pode decidir editar ou não os artigos submetidos, além de sugerir mudanças eventuais, de modo a adequar os textos.

Todos os textos submetidos devem vir acompanhados de Carta de autorização para publicação que garantirá seu ineditismo ou, ainda, que apesar de concorrer a publicação em outras revistas, não está ferindo direitos de publicação com terceiros para ser veiculado nesta publicação.

Outrossim, nenhum dos organismos editoriais, organizações de ensino e pesquisa ou pessoas físicas envolvidas nos conselhos, comitês ou processo de editoração e gestão da revista se responsabilizam pelo conteúdo dos artigos, seja sob forma de ideias, opiniões ou conceitos, devendo ser de inteira responsabilidade dos autores dos respectivos textos.

PERIODICIDADE

A Revista tem a periodicidade anual e se reserva ao direito de realizar edições especiais, além das previstas.

DATA & HERTZ

Revista Científica de
Guerra Eletrônica e Guerra Cibernética
do Centro de Instrução de Guerra Eletrônica

PALAVRAS DO COMANDANTE

É com grande entusiasmo que apresentamos mais uma edição da nossa revista dedicada à disseminação do conhecimento e à promoção da excelência nas áreas de Guerra Eletrônica e Guerra Cibernética. Como estabelecimento de ensino do Exército de referência nessas disciplinas, o Centro de Instrução de Guerra Eletrônica (CIGE) orgulha-se de sua tradição de inovação e capacitação, que perdura há quarenta anos.

Desde 1984, o CIGE vem especializando os recursos humanos da Força Terrestre na área de guerra eletrônica. Foram mais de dois mil e oitocentos militares especializados no CIGE. A partir de 2012, quando passamos a capacitar militares para realizar as ações no espaço cibernético e adicionamos o título de "Berço da Guerra Cibernética" à nossa alcunha de "Alma Mater da Guerra Eletrônica", o CIGE vem desbravando novos horizontes.

Com a evolução da doutrina de Comando e Controle, de Guerra Eletrônica e de Guerra Cibernética do Exército, houve a necessidade de reorganizar e ampliar o Sistema de Comando e Controle da Força Terrestre (SC2FTer), o Sistema de Guerra Eletrônica do Exército (SIGELEX) e o Sistema Militar de Defesa Cibernética (SMDC). Com a criação dos batalhões de comunicações e guerra eletrônica, a demanda por militares capacitados nessas áreas está sendo ainda maior.

Nossa missão é clara: capacitar os recursos humanos necessários para enfrentar os desafios da era digital, contribuindo para a evolução doutrinária por meio de cursos, estágios, atividades de pesquisa e programas de pós-graduação nas áreas de guerra eletrônica e cibernética.

É nesse mister que apresentamos a 3ª edição da revista DATA & HERTZ que visa compartilhar os frutos do esforço intelectual de nossos instrutores e alunos. Apresentamos trabalhos que buscam desmistificar conceitos complexos, oferecendo uma linguagem acessível e atrativa, sem comprometer a profundidade essencial a qualquer produção científica.

Destacamos, com justiça, os militares cujos artigos foram selecionados. São profissionais dotados de um espírito inovador aguçado e que demonstraram elevado interesse pela pesquisa e uma visão de futuro inigualável. Seus trabalhos não apenas enriquecem esta publicação, mas também capturam a atenção tanto de especialistas quanto de leigos, demonstrando a relevância e o impacto das pesquisas desenvolvidas em nosso Centro.

Ao folhear estas páginas, convidamos você a embarcar em uma jornada de descoberta, aprendizado e reflexão. Que esta revista não apenas elucide dúvidas, mas também inspire novos interessados a se juntarem aos nossos especialistas em Guerra Eletrônica e Guerra Cibernética.

Agradecemos a todos os envolvidos por sua dedicação e contribuição, desejando a cada leitor uma experiência de leitura enriquecedora.

Boa leitura!

Tenente-Coronel Com Joselito Rodrigues da Silva

Diretor de Ensino

DATA & HERTZ

Revista Científica de
Guerra Eletrônica e Guerra Cibernética
do Centro de Instrução de Guerra Eletrônica

EDITORIAL

Caro leitor,

Esta nova edição da nossa revista científica dá continuidade a uma das principais missões do nosso Centro, contribuir com a inovação tecnológica divulgando as pesquisas científicas nas áreas de Guerra Eletrônica e Guerra Cibernética.

Com a evolução científico-tecnológica a utilização dos meios digitais de acesso a informação cresceram exponencialmente e com isso a Educação Militar se tornou uma referência no desenvolvimento de atitudes, conhecimentos e habilidades, principalmente aquelas relacionadas a essas tecnologias.

Neste contexto, a pesquisa científica se tornou um dos pilares do desenvolvimento das competências buscadas pelos cursos. Além disso, é uma das principais ferramentas utilizadas na construção das capacidades de análise e de reflexão, além do pensamento crítico. Assim, Data&Hertz pretende fomentar a atividade de pesquisa científica com o objetivo de produzir conhecimento para a evolução doutrinária e para o conteúdo das disciplinas ofertadas pelo Centro.

Além de contribuir para o desenvolvimento de habilidades importantes para a liderança, como a comunicação escrita e a arte de persuasão, um dos nossos maiores desafios é a redação do trabalho científico para a publicação e o domínio do discurso acadêmico pelos militares, peça fundamental para a disseminação do conhecimento nos meios civil e militar.

Ao final desta edição, apresentamos um artigo de opinião, novidade em nosso exemplar de 2023. Esperamos ter contribuído para o desenvolvimento do pensamento crítico militar entregando à sociedade e às Forças Armadas profissionais habilitados e mais competentes, permitindo a evolução da Doutrina Militar Terrestre e o avanço do conhecimento em Defesa.

Tenente-Coronel Com Luciano da Silva
Subdiretor de Ensino

Simulador de Ações Cibernéticas (SACi), o Cyber Range do Exército Brasileiro: preparando as Forças Armadas para os desafios cibernéticos do século XXI.

Major Rodrigo **Rocha** Nunes

RESUMO

O avanço tecnológico e a crescente dependência da Internet e das tecnologias digitais têm impulsionado o desenvolvimento de capacidades cibernéticas em diversas áreas, incluindo a militar. No contexto das Forças Armadas, a cibersegurança tornou-se uma preocupação fundamental, dada a crescente ameaça de ataques cibernéticos a infraestruturas críticas, sistemas de defesa e operações militares. Nesse sentido, a implementação de um Cyber Range para o Exército Brasileiro surge como uma necessidade urgente para preparar suas tropas para enfrentar os desafios cibernéticos do século XXI. Este artigo explora a importância e os benefícios da criação e operação de um Cyber Range eficaz e adaptado às demandas específicas do Exército Brasileiro denominado Simulador de Ações Cibernéticas (SACi) .

Palavras-chave: Cyber Range. Cibernética. Simulador.

Cybernetic Actions Simulator(SACi) Cyber Range of the Brazilian Army preparing the Armed Forces for cyber challenges of the 21st century.

ABSTRACT

Technological advancement and growing dependence on the Internet and digital Technologies have driven the development of cybernetic capabilities in several areas, including the military. In the context of the Armed Forces, cybersecurity has become a key concern, given the growing threat of cyberattacks to critical infrastructure, defense systems, and military operations. In this sense, the implementation of a Cyber Range for the Brazilian Army emerges as an urgent need to prepare its troops to face the cyber challenges of the 21st century. This article explores the importance and benefits of creating and operating an effective Cyber Range, adapted to the specific demands of the Brazilian Army called the Simulator of Cybernetic Actions (SACi).

Keywords: *Electronic Warfare. MAGE NCom. ARP. Radar. Radar Alert.*

Artigo recebido em 31/08/2023 e aceito para publicação em 30/12/2023.

1 INTRODUÇÃO

As guerras do século XXI não serão travadas apenas no campo de batalha físico, mas também nos vastos domínios cibernéticos. A transformação digital trouxe novas oportunidades, mas também aumentou a vulnerabilidade das redes militares a ataques cibernéticos complexos e sofisticados (Avelar, 2018). Nesse contexto, o Exército Brasileiro, responsável pelo setor cibernético das forças armadas, enfrenta o desafio de capacitar suas tropas para defender, atacar e operar no espaço cibernético (Brasil, 2008). Um Cyber Range é uma ferramenta indispensável nessa empreitada, permitindo treinamento em ambientes simulados e realistas.

2 CYBER RANGE E SUA IMPORTÂNCIA

Um Cyber Range é uma infraestrutura de treinamento que simula ambientes cibernéticos realistas, permitindo que as tropas pratiquem suas habilidades de guerra cibernética em condições controladas (KATSANTONIS). Essa abordagem de treinamento oferece uma série de vantagens na preparação das tropas das Forças Armadas.

Soluções de cyber range permitem que profissionais de cibersegurança possam estar preparados para ataques. Longe de nós desmentir o clássico ditado popular de que "a prática leva à perfeição". Quando o assunto é segurança cibernética, a experiência do cotidiano é indispensável e insubstituível para garantir que o profissional do setor saiba lidar com as mais desafiadoras situações de crise. […] (Distrito, 2022)

2.1 REALISMO CONTROLADO

O Cyber Range permite simular cenários complexos e ataques cibernéticos em ambientes seguros e controlados, permitindo aos soldados se familiarizarem com situações reais sem riscos operacionais (NIST).

2.2 TREINAMENTO MULTIDIMENSIONAL

As operações cibernéticas podem ser multifacetadas, envolvendo aspectos técnicos, táticos e estratégicos. O Cyber Range oferece treinamento holístico que abrange diversos níveis de complexidade (NIST).

2.3 AVALIAÇÃO E APERFEIÇOAMENTO CONTÍNUO

Os exercícios no Cyber Range permitem a avaliação do desempenho das tropas, identificando fraquezas e aprimorando habilidades, a fim de fortalecer a resiliência cibernética (NIST).

3 O SIMULADOR DE AÇÕES CIBERNÉTICAS - SACi

O Centro de Instrução de Guerra Cibernética, CIGE, organização militar subordinada ao CCOMGEX, iniciou o desenvolvimento do Simulador de Operações Cibernéticas (SIMOC) 2011, para atender às necessidades do processo de ensino-aprendizagem dos cursos de Guerra Cibernética. Dentre as atribuições de ensino deste Centro, a existência de um ambiente simulado para o ensino das técnicas de ataque, defesa e exploração cibernética, é considerado primordial pelos instrutores do CIGE, tendo em vista que não é viável a utilização de redes em produção, por se tratarem de técnicas que, por vezes, podem comprometer a segurança da informação, dos dados e das comunicações. Sua última atualização ocorreu em 2016, com a inclusão de desafios cibernéticos *capture the flag* no seu código-fonte (CIGE, 2021).

Durante os 10 (dez) anos de utilização do SIMOC, novas capacidades técnicas e procedimentais foram sendo desenvolvidas no ambiente cibernético, o que deixou o simulador descontinuado quanto às principais ações cibernéticas. Ademais, foi observado que o acréscimo de novas funcionalidades sobrecarregaria os processos e poderia extrapolar a sua capacidade de memória, além de ser identificada a incompatibilidade entre os sistemas operacionais que foram instalados na sua última versão, em 2016, e aqueles em uso na atualidade (CIGE, 2021).

Em razão da necessidade de agregar novas funcionalidades e dominar por completo o seu ciclo de vida (CIGE, 2021), a equipe de instrutores e monitores da Seção de Ensino de Guerra Cibernética do CIGE, aproveitando-se do surgimento de novas tecnologias de virtualização e do melhor entendimento acerca dos processos envolvidos em uma simulação cibernética, passou a desenvolver, no ano de 2020, um simulador de ações cibernéticas baseado em tecnologias "open-source", ou seja, com reduzido custo para o Exército Brasileiro, mitigando os problemas que o SIMOC poderia apresentar ao longo do tempo, devido às razões da evolução tecnológica, associada à disponibilidade de recursos de custeio para sua manutenção. Apesar de existirem soluções prontas no mercado, nenhuma delas atendia, plenamente, todas as necessidades do CIGE.

No ano de 2022 foi firmada uma parceria com o Centro de Desenvolvimento de Sistemas, onde aquela OM, reconhecida como uma das Instituições Científicas, Tecnológicas e de Inovação (ICT), passou a dar continuidade ao desenvolvimento do simulador idealizado pelo CIGE sendo assim co-participante da referida invenção (CDS, 2022).

Ainda, naquele ano, visualizou-se parceria com o Instituto Militar de Engenharia ao qual viabilizou a participação de 1 aluno e 1 professor de Engenharia de Software durante 12 meses para o apoio no projeto. A previsão de entrega para o ano de 2023 dos módulos de INSTRUTOR, que permitirá a criação de cenários e organização dos ambientes cibernéticos e do módulo ALUNO, o qual permitirá o acesso ao ambiente controlado, além de contar com o módulo de VPN, o qual permitirá o aluno entrar no ambiente controlado a partir de sua própria máquina (2°CGEO, 2022).

3.1 TECNOLOGIA DESENVOLVIDA

O Simulador de Ações Cibernéticas (SACi) é um sistema de aplicação didática empregado em cursos de capacitação, especialização e extensão que exijam do aluno conhecimentos técnicos na operação de recursos de tecnologia da informação e comunicações em um ambiente de operações cibernéticas no âmbito das Forças Armadas (FA).

O simulador virtualiza o comportamento de uma rede típica, composta de roteadores, switches, firewalls e estações de trabalho. Além disso,

também simula serviços de rede, tais como servidor de correio eletrônico, servidor de páginas (servidor Web), servidor de arquivos, além de simular enlaces de dados, perfis de tráfego de redes, dentre outros serviços de rede existentes no mundo real. As ações desencadeadas pelos alunos têm reflexo no comportamento do ambiente de simulação, a partir de condições e cenários pré-definidos pelos instrutores, de modo que, por meio do emprego de técnicas de virtualização, é capaz de implementar um ambiente estanque no qual os alunos podem conduzir e reproduzir, de forma segura e controlada, ações e situações encontradas no mundo cibernético real.

A página web do SACi serve como uma ferramenta de Área de Trabalho Remota, pois permite conexão SSH, VNC e RDP. Ele funciona como um *gateway* de Desktop Remoto que só precisa ser instalado em um servidor central. Assim, ele fornecerá um painel de controle, baseado na web, que lhe permitirá mudar rapidamente de uma máquina para outra – tudo dentro da mesma janela do navegador.

A página de *login* encontra-se na Figura 1:

Figura 1 – Tela Login

Após realizar o login o aluno é levado a sua própria página onde terá acesso aos ativos que foram virtualizados para seu treinamento, como demonstrado na Figura 2:

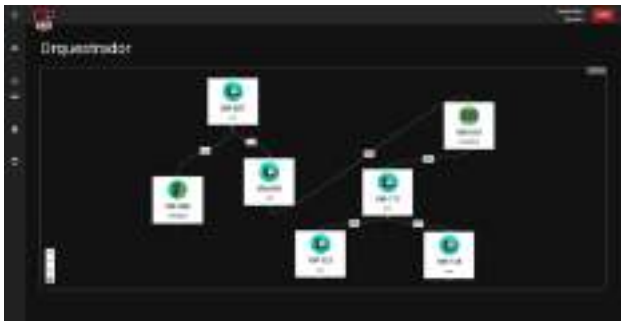
Figura 2 – Tela Atividades

Na Figura 3 imagem podemos ver uma interação do usuário com sua máquina:

Figura 3 – Tela com interação do usuário

Na Figura 4 é possível ver o mapa de rede que é disponibilizado para o aluno, onde através do orquestrador ele tem uma visão mais ampla de sua rede pessoal.

Figura 4 – Mapa da rede



3.2 MÓDULOS

A intenção de se criar em código aberto é a facilidade de novas ideias serem agregadas a plataforma central do SACi, assim já estão sendo desenvolvidos outros módulos como os de CAPTURE THE FLAG, VPN, INFRAESTRUTURAS CRÍTICAS, INTELIGÊNCIA ARTIFICIAL, DEMONSTRAÇÃO DE ATAQUES CIBERNÉTICOS e fomentados por alunos do IME em seus trabalhos de conclusão de curso e dissertação de mestrado, como nos artigos científicos do curso de Guerra Cibernética no CIGE.

Figura 5 – Módulo de infraestruturas

4 BENEFÍCIOS DO SACI PARA O EXÉRCITO BRASILEIRO

A implementação do Simulador de Ações Cibernética (SACi) no Exército Brasileiro oferece uma série de benefícios que impactam positivamente suas operações. A customização é uma das vantagens mais notáveis, pois permite adaptar as funcionalidades do simulador de acordo com as necessidades específicas da Força Terrestre. Com isso, o SACi pode ser ajustado para refletir as políticas, Técnicas, Táticas e Procedimentos (TTP) que serão empregados em suas operações de ciberdefesa.

Além disso, a adoção do SACi apresenta uma solução econômica e escalável para o Exército Brasileiro. Ao contrário da contratação de serviços de terceiros, que pode ser dispendiosa e limitada em termos de flexibilidade, o SACi oferece maior controle sobre o processo de desenvolvimento, teste e implementação. Isso permite ao Exército ter total domínio sobre os dados utilizados, as configurações de simulação e as métricas de desempenho, garantindo a eficácia e a eficiência dos treinamentos.

O SACi também é uma ferramenta eficaz para o treinamento das equipes de exploração, ataque e proteção cibernética. Os membros da equipe podem praticar e aprimorar suas habilidades em um ambiente simulado e seguro, sem expor a Força a riscos desnecessários.

Além disso, a experiência de simulação pode ser personalizada para atender às necessidades individuais de cada membro da Organização Militar (OM), proporcionando um treinamento mais eficiente e ágil.

Outro ponto relevante é que o desenvolvimento do SACi pode estimular a inovação e o pensamento criativo das equipes envolvidas na ciberdefesa. O ambiente simulado permite que as equipes experimentem novas abordagens e testem novas tecnologias antes de aplicá-las em cenários reais, impulsionando a busca por soluções mais avançadas e eficazes.

Outra capacidade fundamental do SACi é a simulação de diferentes cenários de ameaças e a testagem de respostas diversas. Isso resulta em uma tomada de decisão mais informada e embasada, preparando a equipe para lidar com situações reais de ameaça cibernética com maior precisão e efetividade.

Além dos benefícios operacionais, a implementação do SACi também fomenta a colaboração. Nesse contexto, o Instituto Militar de Engenharia (IME), o Centro de Desenvolvimento de Sistema (CDS) e o Comando de Comunicações e Guerra Eletrônica do Exército (CCOMGEX), através do CIGE, trabalham em conjunto para a produção de novos conhecimentos, a promoção da inovação tecnológica e o desenvolvimento no âmbito da ciberdefesa.

5 CONCLUSÃO

A cibersegurança é uma prioridade estratégica para o Exército, e a preparação para os desafios cibernéticos requer uma abordagem holística que inclua o treinamento adequado das tropas.

A implementação de um Cyber Range dedicado ao Exército é uma iniciativa essencial para aprimorar as capacidades cibernéticas e garantir a prontidão para enfrentar as ameaças cibernéticas emergentes. Com investimentos nessa área, o Exército estará melhor preparado para proteger suas redes, defender suas operações e manter a superioridade cibernética nas futuras batalhas. Assim, a implementação do Simulador de Ações Cibernética (SACi) traz uma série de benefícios cruciais para a ciberdefesa do país.

A customização, economia de recursos, controle do processo de desenvolvimento, eficiência no treinamento da equipe, incentivo à inovação, simulação de cenários e a colaboração representam vantagens significativas.

O SACi emerge como uma ferramenta estratégica e imprescindível para fortalecer a cibersegurança e a preparação das Forças Armadas diante dos desafios cada vez mais complexos e dinâmicos do cenário cibernético.

REFERÊNCIAS BIBLIOGRÁFICAS

AVELAR, José Ricardo Cabral. Guerra Cibernética e seus desafios para o Brasil. 2018. 74f. **Trabalho de Conclusão de Curso** (Especialização em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2018. Disponível em: https:// bdex.eb.mil.br/jspui/ bitstream/123456789/2893/1/MO%205894%20-%20AVELAR.pdf. Acesso em: 04 set. 2023.

BRASIL. Centro de Instrução de Guerra Eletrônica (CIGE). **Projeto SACi**, 11 de outubro 2022. Brasília, 2022.

BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. **Aprova a Estratégia Nacional de Defesa**. Brasília, 2008.

BRASIL. Centro de Instrução de Guerra Eletrônica (CIGE). Justificativa para a devolução do recurso e mudança do objeto da licitação do SIMOC. **Memória de Decisão** nº 001/CIGE, 23 de setembro de 2021. Brasília, 2021.

DISTRITO. **Cyber range**: plataforma e solução de simulação de ataques, 3 de março de 2022. Disponível em: https://distrito.me/blog/o-que-e-cyber-range/. Acesso em: 04 ago. 2023.

KATSANTONIS, M. N.; MANIKAS, A.; MAVRIDIS, I.; GRITZALIS, D. Cyber range design framework for cyber security education and training. **International Journal of Information Security**, v. 22, p. 1005-1027, 2023. Disponível em: https://link.springer.com/article/10.1007/s10207-023-00680-4#Sec1. Acesso em: 04 set. 2023.

NIST. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. The Cyber Range: A Guide. Disponível em: https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf. Acesso em: 10 ago. 2023.

Anti-SARP e os desafios para a Guerra Eletrônica

Major Com Bruno **Elias Ribeiro**

RESUMO

O emprego dos sistemas de aeronaves remotamente pilotadas (SARP) em combate trouxe atualizações relevantes para a doutrina militar. No Brasil, seu uso está condicionado à legislação de controle do espaço aéreo. A atuação do Anti-SARP com ações não cinéticas, por sua vez, se destina à proteção das tropas em combate e à segurança de infraestruturas críticas, em especial contra os SARP de Categoria 0 e 1. As Medidas de Ataque Eletrônico, nesse contexto, devem ser traduzidas em táticas, técnicas e procedimentos, constituindo novos desafios para o emprego da Guerra Eletrônica em combate. Além disso, as tecnologias portadoras de futuro ampliam ainda mais esses desafios, realimentando o ciclo de evolução doutrinária e evidenciando ainda mais a importância da capacidade operacional Guerra Eletrônica para a Força Terrestre.

Palavras-chave: SARP. Guerra Eletrônica. Tecnologias futuras.

Counter-UAV and Challennges to Electronic Warfare

ABSTRACT

The use of Unmanned Aerial Vehicles (UAV) in combat brought relevant updates to military doctrine. In Brazil, their use is conditioned by air space control rules. On the other hand, the non-kinetic actions concerning Counter-UAV systems are intended for the protection of surface troops and towards critical infrastructure safety, especially against First Class Unmanned Aerial Vehicle category. This way, Electronic Counter Measures must be translated into tactics, techniques and procedures, performing new challenges for electronic warfare deployment in combat activities. Besides, future-bearing technologies enhance such challenges, reinforcing the doctrinary evolution cycle and further highlighting the importance of Electronic Warfare towards Land Force.

Keywords*:* Counter-UAV. Electronic Warfare. Future technologies.

Artigo recebido em 31/08/2023 e aceito para publicação em 30/12/2023.

1 INTRODUÇÃO

O conflito entre Rússia e Ucrânia teve início no ano de 2022, na madrugada de 23 para 24 de fevereiro, com notícias divulgadas em fontes abertas sobre provedores de internet ucranianos com falhas de conexão e queda dos serviços das redes de telefonia celular em determinadas regiões. Infere-se, a partir de tais notícias, a presença das ações de Guerra Eletrônica (GE) e Guerra Cibernética (GCiber) no início da contenda (Hoje..., 2022).

A GE, todavia, já estava presente no TO muito antes do início do conflito. É conhecido que, desde a anexação da Crimeia, os sistemas de GE russos monitoravam o território ucraniano em diferentes regiões ao longo da fronteira entre os dois países (Kremetnesky, 2019). Desde então, a GE permanece atuante, conforme a expectativa prévia sobre o emprego dessa importante capacidade operativa ao longo do conflito.

As ações perpetradas pelos combatentes russos e ucranianos também trouxeram inovações para o campo de batalha, particularmente no que diz respeito ao emprego de sistemas de aeronaves remotamente pilotadas (SARP) ou veículos aéreos não tripulados (VANT). O uso das *loitering ammunitions* (sistemas de munições remotamente pilotadas – SMRP) consolidou uma nova capacidade para o emprego dos SARP, cujo emprego já se consagrava na vigilância e no reconhecimento de regiões de interesse para ambos contendores. Nas atividades de vigilância, reconhecimento e ataque, por exemplo, VANTs com visão em primeira pessoa (*First Person View Drones*) foram empregados em conjunto com munições termobáricas e munições inteligentes. Também tem sido efetivo, nesse contexto, o emprego conjunto de VANT e artilharia para localização e destruição de alvos (Slyusar, 2023).

Figura 01 – Emprego de VANT com visão em primeira pessoa no conflito Rússia-Ucrânia

Fonte: Slyusar, 2023.

Essas ações têm sido divulgadas em redes sociais distintas, de forma a potencializar seu efeito psicológico sobre os combatentes e afetar positiva ou negativamente o moral das tropas.

As Organizações Militares (OM) de GE, no âmbito do Exército Brasileiro, têm condições de fazer frente, com limitações, às ameaças impostas pelos drones, como são comumente conhecidos os SARP, empregando para tal as capacidades não cinéticas de suas subunidades de guerra eletrônica. As Técnicas, Táticas e Procedimentos (TTP) referentes ao emprego da capacidade Anti-SARP por meios não cinéticos no âmbito da Força Terrestre serão definidos em Caderno de Instrução a ser difundido pelo Comando de Operações Terrestres.

Este artigo apresentará, no seu desenvolvimento, aspectos referentes ao emprego do SARP e do Anti-SARP no Exército Brasileiro, restringindo o estudo aos drones de categoria (Catg) 0 e 1, mais vulneráveis às ações não cinéticas passíveis de emprego pela GE. Para tal, mencionará conhecimentos presentes em publicações de interesse para a doutrina que tratam do assunto em questão. Por fim, na conclusão, destacará assuntos de interesse para o prosseguimento dos estudos na doutrina Anti-SARP que estão relacionados à GE, e que por seus avanços no domínio científico-tecnológico, certamente trarão relevância para a consecução das operações multidomínio nos conflitos modernos.

2 DESENVOLVIMENTO

No âmbito da Força Terrestre, os SARP podem ser empregados por diversos escalões. São partes constituintes de um SARP categoria 0, por exemplo (Exército Brasileiro, 2021):

a. plataforma aérea, contendo grupo motopropulsor, sistema elétrico e sistema de navegação e controle embarcados;

b. carga útil, composta de sensores e equipamentos embarcados na plataforma aérea, como câmeras de sensores eletro-ópticos e infravermelhos;

c. estação de controle de solo, que é responsável pela interface entre o operador, a plataforma aérea e a carga útil; e

d. terminal de transmissão de dados, com equipamentos que possibilitam os enlaces entre a plataforma aérea e a estação de controle de solo, servindo ao controle do voo e ao controle da carga útil.

As ICA 100-40/2023 (Força Aérea Brasileira, 2023) constituem a legislação de amparo para a coordenação de emprego do espaço aéreo por tais dispositivos. Abrangem, em seu conteúdo, as principais normas para o emprego de SARP de todas as categorias, bem como as sanções previstas para o descumprimento do que se relaciona à segurança no emprego de tais dispositivos.

Em linhas gerais, dentre outras prescrições, aeronaves não tripuladas, com peso máximo de decolagem de até 25kg, operando em linha de visada visual com o operador e até 120m de altura:

a. estão dispensadas do uso de *transponder*;

b. estão dispensadas dos requisitos de funcionamento e desempenho dos sistemas de comunicação, vigilância e navegação para seus sistemas de forma equivalente aos estabelecidos para aeronaves tripuladas;

c. devem possuir luzes que possibilitem sua visualização à noite, sem contudo atender aos mesmos requisitos previstos para aviação tripulada; e

d. devem ter sua operação encerrada ao aproximar-se de aeronaves tripuladas ou SARP operado por órgão de segurança pública (OSP).

Figura 02 – Categorização de SARP empregada pela OTAN e pelo Exército Brasileiro

Fonte: Exército Brasileiro, 2023.

Verifica-se no quadro apresentado na Figura 02, por exemplo, que os SARP Categoria 0 e 1, objetos de estudo do presente artigo, estão abrangidos pelas prescrições anteriormente citadas. É provável que os SARP Catg 1 sejam priorizados para Brigadas Leves de Emprego Estratégico (Amv, Pqdt, Mth, Sl) e grandes comandos assemelhados, sendo os SARP Catg 0 descentralizados às unidades empregadas em 1º escalão, como Batalhões e Regimentos (Exército Brasileiro, 2023[a]).

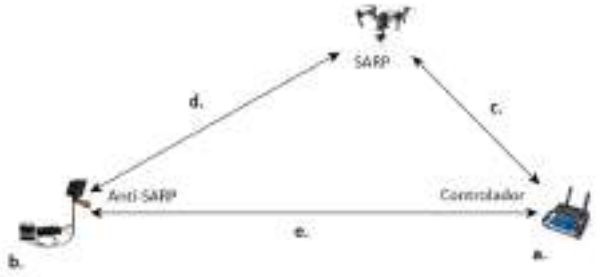
Além das prescrições anteriormente citadas nas ICA 100-40/2023, quando a operação do SARP ocorrer sobre áreas de segurança, como: refinarias; depósitos de combustíveis; áreas militares; sedes de governos; instalações hidroelétricas, termoelétricas ou nucleares; redes de abastecimento de água ou gás; barragens ou represas; redes de comunicação, como sítios de antenas; redes de vigilância da navegação aérea, como radares de vigilância aérea. Instalações que, quando danificadas provocam sério impacto social, político, econômico ou à segurança, seu operador estará sujeito às implicações civis e criminais pertinentes. Em alguns casos, está prevista e autorizada a neutralização do SARP quando se tratar de ameaça a tais estruturas críticas (Força Aérea Brasileira, 2023).

Para fazer frente a tais ameaças, especificamente dos SARP categorias 0 e 1, que têm menores dimensões e, por conta disso, têm menor custo e são de mais difícil detecção, diversas tecnologias embarcadas em sistemas Anti-SARP com atuadores não cinéticos podem ser empregadas. Existe a possibilidade do uso de atuadores portáteis para assegurar a autoproteção da tropa, dispositivos mais robustos para a segurança de determinada área, bem como a combinação de meios radar, acústicos e de eletrônica para a detecção e identificação da ameaça SARP (Exército Brasileiro, 2023[a]).

Nos conflitos em andamento, por exemplo, verifica-se preferência no emprego de SARP civis em detrimento dos militarizados, justamente por conta da facilidade em adquirir tal meio e da facilidade de reposição. Contudo, a operação desses dispositivos pode ser comprometida pela GE oponente. (Exército Brasileiro, 2023[a]).

Nesse contexto, o Exército Brasileiro vem conduzindo, por meio do Comando de Operações Terrestres, experimentações doutrinárias referentes ao emprego do Anti-SARP.

Figura 03 – Representação das variáveis que afetam a efetividade das ações não cinéticas sobre os SARP



Fonte: Exército Brasileiro, 2023[b].

Conforme o diagrama apresentado na Figura 03, verifica-se que as seguintes variáveis, descritas a seguir e discriminadas pelas letras de "a" a "e", são determinantes para a efetividade de uma ação Anti-SARP, constituindo desafios para o emprego das ações de GE:

a. A potência do sinal de controle do operador do SARP;
b. A potência do MEM empregado como Anti-SARP não cinético;
c. A distância entre o SARP e o seu operador;
d. A distância entre o SARP e o Anti-SARP não cinético; e
e. A distância entre o controlador do SARP e o Anti-SARP não cinético.

Foram feitos testes contra a capacidade de controle, de transmissão de vídeo e contra o sistema de GPS do SARP, tanto para SARP Catg 0 como SARP Catg 1, que não apresentaram bloqueio efetivo para o emprego de antenas omnidirecionais. Os resultados obtidos nos testes foram registrados em documento de dados médios de planejamento (DAMEPLAN), restrito ao 1º BGE para fins de emprego.

Além das TTP a serem detalhadas pelo Caderno de Instrução Anti-SARP, que será aprovado até o fim do corrente ano, é conveniente destacar novas tecnologias que podem contemplar o emprego do SARP em conflitos vindouros.

São desafios para a guerra eletrônica, uma vez que demandam aprofundamento nas áreas relacionadas ao controle do SARP, principal alvo das ações não cinéticas, de forma a levantar suas vulnerabilidades e propor o meio mais eficaz para o emprego do Anti-SARP.

A primeira a ser citada está relacionada ao emprego da tecnologia de RF em Fotônica (MWP – *Microwave Photonics*), mais especificamente nos enlaces *Free Space Optics (FSO)*, viabilizando links mais direcionais, menos suscetíveis a interferência, para o controle dos drones a curtas distâncias.

Figura 04 – Representação para os enlaces possíveis com o emprego de FSO

Fonte: Kumar & Sharma, 2022.

Na Figura 04, é possível visualizar, por meio das setas entre as imagens de aplicações militares ali representadas, as posições onde é viável o emprego da tecnologia FSO, com destaque para os enlaces entre um posto de comando e um SARP, indicado na figura como UAV – *Unmanned Aerial Vehicle,* e enlace entre dois SARP. Nesse último caso, também seria viável um enlace entre drones integrantes de um enxame (Kumar, 2022). As características inerentes a um sistema que se beneficia do emprego da RF em Fotônica, como a diretividade de um enlace que emprega FSO, podem ser revisadas em Ribeiro (2020).

Outra tecnologia desafiadora para as ações Anti-SARP com emprego de ações não cinéticas por parte da GE consiste no emprego de drones em formação de enxame. Uma dissertação de mestrado da *Naval Postgraduate School* valida simulações computacionais para o emprego da sequência de Zadoff-Chu (utilizada em redes de comunicações 5G), de forma a carregar informações sobre a identificação e o posicionamento de drones em formação de enxame (Martins, 2021). Como afetar tal algoritmo para exercer o controle sobre a movimentação de um enxame de drones?

Por fim, vale citar a Inteligência Artificial (IA), que tem se inserido de maneira significativa no nosso cotidiano e que, com as técnicas de aprendizado de máquina, tem eliminado diversos trabalhos mecânicos anteriormente realizados pelo homem.

Tal tecnologia ainda tem muitas possibilidades a acrescentar ao controle dos SARP, viabilizando sua maior autonomia e consequente independência da atuação de operadores em solo, dependendo da tecnologia embarcada em tais plataformas. Visualiza-se um recente aumento de depósitos de patente e de artigos científicos tanto para a detecção e identificação de SARP inimigos como para a inteligência de enxame, indicativos de que o uso da IA nesse contexto trará consequências a longo prazo (Guimarães et al, 2021).

Assim, foi possível descrever de forma sucinta de que forma os SARP e o emprego do Anti-SARP estão presentes junto a Força Terrestre, bem como as principais tecnologias portadoras de futuro podem ser desafiadoras para o emprego da GE nesse contexto. O estudo sobre os SARP e as tecnologias Anti-SARP deve estar em constante acompanhamento, mantendo a Força Terrestre apta ao emprego dessas capacidades necessárias ao combate moderno.

3 CONSIDERAÇÕES FINAIS

O emprego do SARP como MEM trouxe consequências relevantes para a doutrina de emprego em combate, mobilizando a dimensão informacional, afetando o moral das tropas em combate e externando novos desafios para a capacidade operativa de guerra eletrônica.
Verificou-se no artigo que, para o emprego de SARP Catg 0 e 1, existe uma legislação específica para garantir a segurança do espaço aéreo durante as operações. A mesma documentação prevê a possibilidade de neutralização da ameaça SARP em casos específicos, garantindo a segurança de infraestruturas críticas e áreas militares.

Para eliminar tais ameaças, a Força Terrestre vem conduzindo experimentações doutrinárias empregando atuadores não cinéticos contra os SARP Catg 0 e 1.

Além dos desafios visualizados relacionados ao estabelecimento da atuação do Anti-SARP, foram citadas outras tecnologias portadoras de futuro que moldarão as ações de GE para a efetividade na segurança das tropas e das infraestruturas críticas. Outras tecnologias serão necessárias para fazer frente aos enlaces FSO para controle do drone, bem como ao emprego de formações de drone em enxame, inclusive com a utilização de Inteligência Artificial.

Por fim, é possível confirmar que as constantes evoluções tecnológicas prosseguirão na consolidação de novos desafios para as ações de guerra eletrônica. As mesmas evoluções permitirão, gradativamente, a atualização doutrinária e a adoção de novas TTP para o sucesso das ações de guerra eletrônica em combate.

Por fim, é possível confirmar que as constantes evoluções tecnológicas prosseguirão na consolidação de novos desafios para as ações de guerra eletrônica. As mesmas evoluções permitirão, gradativamente, a atualização doutrinária e a adoção de novas TTP para o sucesso das ações de guerra eletrônica em combate.

REFERÊNCIAS BIBLIOGRÁFICAS

EXÉRCITO BRASILEIRO. Comando de Operações Terrestres. **Minuta do Caderno de Instrução Anti-SARP**. Brasília, 2023[b].

EXÉRCITO BRASILEIRO. Comando de Operações Terrestres. **Relatório do I Seminário Internacional de Doutrina Militar Terrestre**. Brasília, 2023[a].

EXÉRCITO BRASILEIRO. Estado-Maior do Exército. Requisitos Operacionais Sistema de Aeronaves Remotamente Pilotadas Categoria 0 (SARP CATG 0): **EB20-RO-04.052**, 1ª Edição. Brasília, 2021.

FORÇA AÉREA BRASILEIRA. Departamento de Controle do Espaço Aéreo. Aeronaves Não Tripuladas e o Acesso ao Espaço Aéreo Brasileiro: **ICA 100-40**. Rio de Janeiro, 2023.

GUIMARÃES, R. W. A., FERNANDES, L. L., & Madeu, F. C. B. Prospecção Tecnológica: **Tendências e Visão de Futuro em Sistemas Anti-SARP**. Informativo Antiaéreo: publicação científica, (V.13, n.13, p. 35-56). Rio de Janeiro, 2022.

HOJE no Mundo Militar. Praticamente todos os provedores de internet na Ucrânia estão apresentando problemas de conexão. 22 FEV. 2022. **Canal do Telegram**. Disponível no Canal Hoje no Mundo Militar.

Kremetnesky, Borys. ***Russian Hybrid Warfare in Ukraine***. Apresentação aos alunos da ECEME – Rio de Janeiro, RJ.

KUMAR, S., & SHARMA, N. Emerging Military Applications of Free Space Optical Communication Technology: A Detailed Review. In ***Journal of Physics: Conference Series*** **(V. 2161, n. 1, p. 012011). IOP Publishing, 2022.**

Martins, M. A. **5G inspired method for ranging of UAVs in swarming composition**. 88 f. 2021. Thesis (Master of Science in Eletrical Engineering) - Naval Postgraduate School , California USA, 2021.

RIBEIRO, B. E. Aplicação operacional da RF em fotônica. **Data & Hertz**, 1 (V.1, n.1, jan./dez 2020, p. 26-33). Brasília, 2020.

SLYUSAR, Vadyn (2023). *Ukraine: Lessons learned in the context of Armored Vehicles*. **Relatório do EME sobre a *Armored Vehicles Conference***, realizada em Austin-Texas, EUA, em 21 e 22 de junho de 2023. Proceedings.

Aplicação de *beamforming* como técnica anti-*jamming* em receptores ADS-B

Primeiro-Tenente (MB) Michel Salviano **Rivera**

RESUMO

A evolução do controle do tráfego aéreo reflete o amadurecimento da aviação ao longo do tempo. Diante das demandas crescentes por harmonização e interoperabilidade, órgãos especializados foram estabelecidos para regular e padronizar a gestão do tráfego aéreo. O produto emblemático desses esforços é o sistema *Automatic Dependent Surveillance-Broadcast* (ADS-B), usado tanto na aviação civil quanto militar. Em que pesem os avanços significativos em proveito da consciência situacional no espaço aéreo, tornam-se frequentes os questionamentos acerca da susceptibilidade do ADS-B a Medidas de Ataque Eletrônico do tipo *jamming*. No âmbito militar, essas interferências exigem soluções capazes de assegurar o uso eficiente do espectro eletromagnético pela própria Força, dentre as quais se destaca o *beamforming*, pela possibilidade de otimização da diretividade de um arranjo de antenas. Diante do exposto, a presente pesquisa examinou conceitos e conduziu experimentos que pudessem fundamentar a argumentação que respondeu à pergunta nevrálgica do estudo: em que medida o emprego de técnicas de *beamforming* em receptores ADS-B sujeitos a Medidas de Ataque Eletrônico do tipo *jamming* seriam eficientes? A metodologia utilizada foi o método dedutivo, com finalidades exploratórias, valendo-se das técnicas de pesquisa bibliográfica e experimental. Por fim, concluiu-se que há indícios de que a técnica de *beamforming* utilizando o algoritmo *Linear Constrained Minimum Variance* (LCMV) seria eficiente contra efeitos adversos causados pelo *jamming*, em virtude da robustez apresentada face à progressão de complexidade dos ambientes operacionais e da manutenção do parâmetro de taxa de bits errados estatisticamente abaixo do nível correspondente ao corrompimento arbitrário de mensagens ADS-B.

Palavras-chave: ADS-B. Medidas de Ataque Eletrônico. *jamming*. *beamforming*. LCMV.

Application of beamforming as na anti-jamming technique

ABSTRACT

The evolution of air traffic control reflects the maturing of aviation over time. Specialized bodies have been established to regulate and standardize air traffic management in response to increasing demands for harmonization and interoperability. The main product of these efforts is the Automatic Dependent Surveillance-Broadcast (ADS-B) system, used in both civil and military aviation. Despite significant advances in favor of situational awareness in airspace, questions arise about the susceptibility of ADS-B to Electronic Attack Measures such as jamming. In the military context, these interferences require solutions for the Force to use the electromagnetic spectrum efficiently. beamforming stands out for the possibility of optimizing the directivity of an antenna array. This research studied concepts and conducted experiments to answer the pivotal question of the study: How effective are beamforming techniques in ADS-B receivers when faced with jamming? The methodology used was the deductive method for exploratory purposes, using bibliographic and experimental research techniques. Finally, it was concluded that there is evidence that the beamforming technique using the Linear Constrained Minimum Variance (LCMV) algorithm would be efficient against adverse effects caused by jamming due to the robustness presented in the progression of the complexity of operational environments and the maintenance of the wrong bit rate parameter statistically below the level corresponding to arbitrary corruption of ADS-B messages.

Keywords*: ADS-B. Electronic Attack Measures. jamming. beamforming. LCMV.*

Artigo recebido em 31/08/2023 e aceito para publicação em 30/12/2023.

1 INTRODUÇÃO

A evolução do controle do tráfego aéreo é um reflexo notável do desenvolvimento da aviação ao longo do tempo. Com o aumento da quantidade de aeronaves e da complexidade das operações aéreas, surgia a necessidade inequívoca de controlar o tráfego aéreo de forma mais segura e eficiente. Nesse sentido, diversos órgãos especializados foram concebidos, com o intuito de sistematizar o controle do tráfego aéreo por meio de normas e regulamentos.

Diante dos esforços progressivos pela harmonização e interoperabilidade, surgem iniciativas de vanguarda, a fim de liderar a revisão global do sistema de aviação e de gestão do tráfego aéreo. O sistema de comunicação e vigilância em implementação e representante da evolução do controle do tráfego aéreo recebe o nome de *Automatic Dependent Surveillance-Broadcast* (ADS-B)[1], utilizada no âmbito civil e militar para fornecer informações sobre posição, velocidade, altitude e identificação de aeronaves em tempo real.

O ADS-B é caracterizado pela comunicação em radiodifusão, o que significa que as mensagens são transmitidas de forma ampla e indiscriminada, facilitando a captura desses sinais por qualquer receptor dentro do alcance. Se por um lado essa característica provê vantagens significativas à consciência situacional no espaço aéreo, por outro lado, constitui uma vulnerabilidade, facilitando as explorações acintosas desses sinais, diante da carência de mecanismos de segurança.

Dentre as diversas modalidades de ataque, o *jamming* é uma técnica potencialmente danosa à disponibilidade do sinal de interesse, que não exige elevado grau de complexidade na sua implementação. Dessa forma, o presente trabalho analisa o resultado da aplicação da técnica *beamforming*[2] na otimização da diretividade de um arranjo de antenas.

Em um conflito, ser surpreendido por ataques em decorrência de uma consciência situacional deficiente pode gerar resultados catastróficos, com perdas de material e pessoal, podendo influenciar decisivamente no resultado de uma operação militar. Diante disso, existe a necessidade de utilização segura do sistema ADS-B por meios militares, de forma a prover a compilação confiável do quadro tático aéreo. Para tanto, são constantes as buscas pelo desenvolvimento e aperfeiçoamento de técnicas capazes de assegurar o uso eficiente do espectro eletromagnético pela própria Força.

Face ao exposto, esta pesquisa responde à seguinte questão central: em que medida o emprego de técnicas de *beamforming* em receptores ADS-B sujeitos a Medidas de Ataque Eletrônico do tipo *jamming* seriam eficientes?

A relevância desta pesquisa reside na apreciação de métodos de contraposição a possíveis interferências em receptores ADS-B, comparando diferentes modalidades do *beamforming* e analisando-as em termos de adequação ao ambiente operacional aéreo. Assim, este estudo coopera com a construção de conhecimento acerca do ADS-B e das soluções para mitigação de possíveis vulnerabilidades que afetem a disponibilidade do sinal.

O objeto de pesquisa é o comportamento de diferentes aplicações do *beamforming* em ambientes operacionais aéreos progressivamente complexos a partir das simulações. Nesse sentido, a pesquisa tem como proposição analisar o emprego de técnicas de *beamforming*, como medidas anti-*jamming* em receptores ADS-B.

Para tal propósito, utilizou-se da pesquisa experimental para analisar a possibilidade de emprego de técnicas de *beamforming* como método anti-*jamming* em receptores ADS-B. Os dados utilizados foram coletados e exportados para os *softwares* MATLAB 2023b e *Simulink.* Por fim, os resultados obtidos foram apresentados graficamente no domínio do tempo e ratificados sob uma abordagem estatística. Como metodologia, empregou-se o método dedutivo, com finalidades exploratórias, valendo-se das técnicas de pesquisa bibliográfica e experimental.

2 ADS-B: EVOLUÇÃO, CARACTERÍSTICAS E VULNERABILIDADES

Considera-se fundamental o entendimento acerca da evolução do controle do tráfego aéreo, dos sensores primários e do surgimento do ADS-B como método primário de vigilância aérea. A partir dessa contextualização, é possível descrever as características gerais do sinal transmitido e as vulnerabilidades inerentes a essa tecnologia, proporcionando uma visão geral da mitigação dessas lacunas de segurança, com foco no conceito de *beamforming*.

1 ADS-B - Vigilância Dependente Automática por Radiodifusão.

2 O termo *beamforming*, em tradução livre, significa formação de feixes.

2.1 EVOLUÇÃO DO CONTROLE DO TRÁFEGO AÉREO

A evolução do controle do espaço aéreo tem sido marcada por avanços tecnológicos significativos que visam tornar o sistema mais seguro, eficiente e sustentável frente aos desafios atuais (Aireon, 2023). Esse aspecto motiva a atuação de órgãos especializados, cujos papéis se mostram progressivamente importantes. Nesse contexto, observa-se os papéis preponderantes da Organização da Aviação Civil Internacional (ICAO), a nível global, e da Administração Federal de Aviação (FAA) e da Organização Europeia para a Segurança da Navegação Aérea (EUROCONTROL), a nível nacional e regional.

Assim surge a *NextGen,* uma revisão global do sistema de aviação dos EUA e uma evolução da gestão do tráfego aéreo. A quantidade de colaborações mútuas entre órgãos e países são indícios da importância dada pela comunidade aeronáutica à padronização e consolidação dessas novas tendências, ou seja, da busca por maior interoperabilidade de aviônicos, protocolos de comunicações e métodos operacionais (USA, 2020).

A FAA fomenta o desenvolvimento de sistemas facilitadores essenciais que melhorem as comunicações, a navegação, a vigilância, o fluxo de tráfego e a automatização do apoio à decisão. O estandarte desses estímulos é dado pelo amadurecimento da infraestrura *Automatic Dependent Surveillance-Broadcast* (ADS-B). O ADS-B é uma tecnologia de comunicação e vigilância usada na aviação civil e militar para fornecer informações precisas sobre a posição, velocidade, altitude e identificação de aeronaves em tempo real. O resultado é a transmissão automática de informações para aeronaves e estações terrestres, melhorando a eficiência, segurança e capacidade do controle de tráfego aéreo (Aireon, 2023).

Vieira (2018) contextualiza que o tráfego aéreo foi tradicionalmente marcado pela simbiose entre Radares de Vigilância Primários (PSR) e Secundários (SSR). Os PSR são sensores consagrados de detecção pela reflexão de ondas eletromagnéticas e são, sobretudo, independentes de qualquer cooperação por parte do contato de interesse. Parâmetros como distância, marcação e velocidade são obtidos pelo PSR. Os SSR, por sua vez, utilizam-se do mecanismo de interrogação para obter informações precisas de altitude, identificação ou até mesmo de problemas técnicos. A interrogação consiste no envio de mensagens pela unidade transmissora para alvos dotados de transponders habilitados a responder a partir dos dados codificados.

Strohmeier et al. (2014) lembram que, antes do ADS-B, todos os SSR eram baseados na interrogação. O ADS-B, como tecnologia, é uma atualização dos SSR e, em termos de mensagens, é uma evolução do Modo S de interrogação. A diferença fundamental entre o ADS-B e o Modo S é a capacidade de transmissão em radiodifusão, sem fazer uso dos reconhecidos mecanismos de interrogação. Outro aspecto relevante é relacionado à frequência: nos modos anteriores, a interrogação era feita na frequência de 1030 MHz e a resposta, na de 1090 Mhz. Na tecnologia ADS-B, a frequência de 1030 MHz não se faz mais necessária.

O incremento da consciência situacional é apresentado por Strohmeier *et al*. (2014) como um efeito crucial do emprego do ADS-B pelas aeronaves na transmissão automática de localização e intenção de movimento. Naturalmente, a harmonização e a implementação global dessa tecnologia contribuirão diretamente na sua efetividade em larga escala. Para tanto, há um visível aumento dos esforços dos Estados em prol da regulamentação do ADS-B, ainda que em diferentes estágios de concretização.

Os EUA se apresentam no estado da arte quanto à implementação do sistema em larga escala. Desde 2020, encontra-se em vigor a obrigatoriedade de implantação do ADS-B por todos os usuários (CERQUEIRA, 2021). A União Europeia, por sua vez, possui diretrizes muito semelhantes às estadunidenses, cuja determinação do emprego do ADS-B por novas aeronaves se encontra em vigor desde 2020 e até junho de 2023 todas as aeronaves deveriam estar adaptadas. O Brasil, por sua vez, encontra -se nos estágios iniciais de implementação. No entanto, observam-se os esforços das principais entidades no contexto da aviação e do controle de tráfego aéreo, a saber, o Departamento de Controle do Espaço Aéreo (DECEA) e a Agência Nacional de Aviação Civil (ANAC), de forma que o sistema ADS-B de vigilância do espaço aéreo continental brasileiro seja gradativamente implantado até o segundo semestre de 2026 (COMAER, 2023a).

2.2 CARACTERÍSTICAS BÁSICAS

O ADS-B, que é considerado como uma tecnologia de vigilância dependente cooperativa, possibilita o incremento na capacidade de

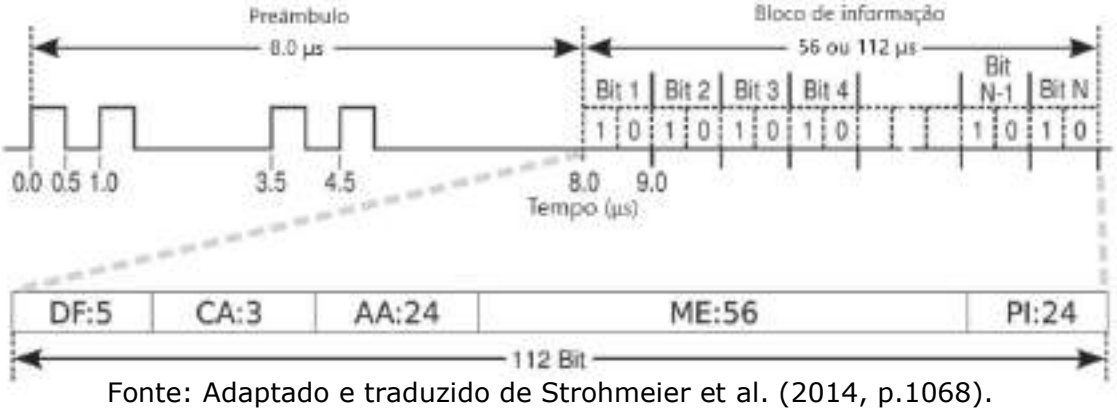
vigilância dependente cooperativa, possibilita o incremento na capacidade de vigilância, ao passo que reduz custos de manutenção e instalação observados nos sistemas de vigilância antecessores (Abdulaziz *et al*., 2015). Outro diferencial proposto pelo ADS-B é a habilitação de estações terrestres para operação em áreas outrora inimagináveis, como o espaço aéreo oceânico e áreas montanhosas (Galati *et al*., 2002).

O acrônimo ADS-B facilita a sua própria distinção como tecnologia de vigilância: o termo *Automatic* deriva da capacidade de transmissão de informações sem qualquer interrogação; *Dependent*, da necessidade de contar com fontes de navegação e outros subsistemas para provimento de informações de vigilância; *Surveillance*, do provimento de informações das aeronaves pelo *Global Navigation Satellite System* (GNSS), e *Broadcast*, do recebimento de dados por qualquer receptor ADS-B dentro do alcance (USA, 2017).

A operação do ADS-B é categorizada em duas partes distintas, conhecidas por ADS-B OUT e ADS-B IN (Strohmeier et al., 2014). Instalado nas aeronaves, o ADS-B OUT realiza a transmissão em radiodifusão das informações. O ADS-B IN, por sua vez, é o "braço receptor" do sistema, que permite a quaisquer usuários receber os dados transmitidos pelo ADS-B OUT (USA, 2017). O ADS-B, em termos de mensagem, está encapsulado em um quadro de resposta do Modo S. A transmissão ADS-B é composta por duas divisões, a saber, preâmbulo e bloco de dados, conforme mostrado na Figura 1.

De acordo com Strohmeier et al. (2014), a transmissão do bloco de dados é iniciada 8 µs após o início do primeiro pulso do preâmbulo. A taxa de transmissão de bits é de 1 Mbps, utilizando modulação por posição de pulso (PPM). O quadro de resposta ADS-B é composto por 112 bits, divididos em cinco campos, descritos no Quadro 1.

Figura 1: Quadro de resposta ADS-B



Fonte: Adaptado e traduzido de Strohmeier et al. (2014, p.1068).

Quadro 1 : Campos do bloco de dados de uma transmissão ADS-B

Campo	Nº de *bits*	Descrição
Downlink Format (DF)	5	Definição do tipo de quadro. No caso do ADS-B, o downlink é igual a 17 (10001 em binário)
Capability (CA)	3	Envio das capacidades do transponder utilizado pela aeronave em relação à transmissão de informações
Aircraft Address (AA)	24	Identificação única fornecida por autoridades homologadas pela ICAO
Message (ME)	56	Transmissão de mensagem com parâmetros definidos em DF
Parity (PI)	24	Verificação de integridade e detecção de possíveis erros de transmissão, pela técnica *de Verificação Cíclica de Redundância* (CRC). Pode corrigir até 5 bits, mas qualquer mensagem com erros maiores é considerada uma mensagem corrompida e descartada

Fonte: Elaborado pelo autor, a partir de informações extraídas de Strohmeier et al. (2014, p. 1067-1068) e Vieira (2018, p. 32).

2.3 VULNERABILIDADES

A comunicação por radiodifusão é uma característica fundamental do ADS-B. Esse padrão evidencia a transmissão indiscriminada de mensagens pelos equipamentos transmissores ADS-B, ou seja, qualquer usuário dotado de um receptor ADS-B pode ter acesso a essas informações, desde que dentro do alcance (Mccallie et al., 2011). Assim, observa-se um perigoso precedente: em que pese a vantagem da transmissão em tempo real, é possível que usuários quaisquer explorem as comunicações de maneira maliciosa em caso de insuficiência de mecanismos que garantam sua segurança. Kim, Jo e Lee (2017) expõem a falta de mecanismos adicionais que corroborem a localização da aeronave em caso de falhas, provocadas ou não, e trazem à tona preocupações sobre a confiança do atual sistema primário de vigilância radar dos EUA, cujas questões podem reduzir drasticamente a efetividade do controle de tráfego aéreo , caso não sejam resolvidas.

É possível sugerir que os desafios de prover segurança e eficiência ao espaço aéreo não seriam tão complexos caso a variável militar não se fizesse presente. Aeronaves militares, tripuladas ou não, fazem parte de um ecossistema que não pode ser dissociado da aviação civil. Aspectos como a consciência situacional, a separação de altitudes e o tráfego aéreo dependem de uma estrutura de controle integrada. No entanto, certas vulnerabilidades não poderiam sequer ser admitidas por um meio militar, como posição e intenções de movimento. Leite Junior (2021) aponta que essa premissa militar crítica decorre da crescente importância conferida à utilização das ondas eletromagnéticas e do papel crucial assumido nas esferas estratégica, operacional e tática das ações militares, ou seja, na Guerra Eletrônica (GE) em si.

Dentre todas as formas de suavizar a susceptibilidade do ADS-B a ataques, é compreensível, no âmbito da Proteção Eletrônica, dar enfoque ao estudo de técnicas anti-*jamming*. O *jamming* é uma modalidade de ataque de menor complexidade de implementação, sem a necessidade de uso de técnicas mais sofisticadas e, ainda assim, causa danos significativos à disponibilidade do sinal (Manesh; Kaabouch, 2017). A diversidade de estratégias e tipos de bloqueio também deve ser considerada, podendo ser muito eficaz como fator de ocultação de um ataque primário, por exemplo (McCallie et al., 2011).

Faz-se necessário buscar soluções de maior abrangência e menor complexidade de implementação. As Forças Armadas brasileiras, por exemplo, são agentes potencialmente interessados no incremento da capacidade de compilação do tráfego aéreo, aliado à eficácia na contraposição a possíveis ataques eletrônicos.

Nesse contexto, Balasem, Tiong e Koh (2012) destacam o *beamforming*, princípio consagrado da área de processamento de sinais utilizado na otimização da diretividade do sinal proveniente de um arranjo de antenas. Ao invés de transmitir ou receber o sinal em todas as direções, o *beamforming* permite ajustar as fases e amplitudes dos sinais transmitidos ou recebidos por várias antenas para formar um feixe direcionado. O efeito desejado é a concentração da energia do sinal na direção de interesse enquanto minimiza a energia capturada em outras direções.

2.4 *BEAMFORMING*

O conceito de *beamforming*, conforme introduzido anteriormente, é digno de aprofundamento à medida que sugere, a priori, incrementos significativos na capacidade de detecção seletiva por receptores. Van Trees (2002) enumera uma série de componentes que torna o sistema de formação de feixes apto a alcançar o seu efeito desejado, quais sejam: arranjo de antenas, matriz de covariância e os tipos de *beamforming*, em função do ajuste de pesos.

O arranjo de antenas compõe a base física do *beamforming*, desempenhando papel fundamental na coleta de sinais. O seu ajuste possui estreita relação com a capacidade de suprimir sinais indesejados. A matriz de covariância, por sua vez, encarrega-se de fornecer informações estatísticas entre os sinais recebidos de cada antena aos algoritmos de ajuste de pesos, descritos a seguir, e aos algoritmos de estimação da Direção de Chegada (DOA – *Direction Of Arrival*).

O ponto nevrálgico do presente artigo reside no tipo de técnica de *beamforming* empregado: a ele é atribuída a tarefa de otimizar a configuração das antenas e definir a forma como a energia do sinal é direcionada. O *beamforming* pode ser classificado em *convencional* ou *adaptativo.*

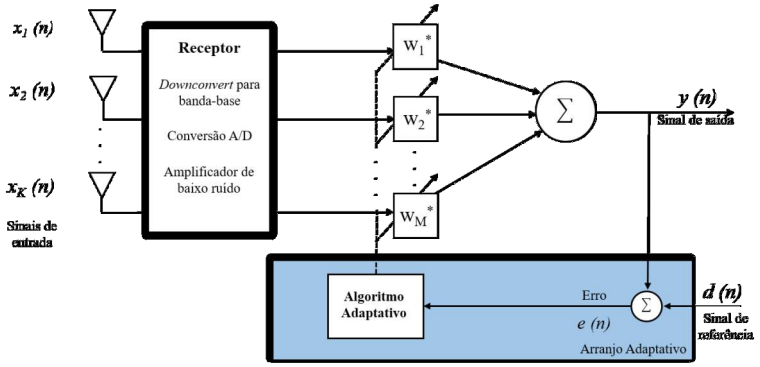
O *beamforming* convencional possui uma abordagem estática e, portanto, não adaptativa. Em virtude disso, sugere-se que esse método seja aplicado em situações em que a DOA do sinal de interesse não varie com o tempo, pressupondo que haja conhecimento ou algum grau de estimativa quanto à DOA do sinal desejado. O presente trabalho, por ocasião das simulações, analisa a técnica conhecida por *Phase Shift Beamformer*, dentre

as essencialmente convencionais. Trata-se de uma abordagem simples em que os sinais recebidos pelas antenas são ajustados em fase pelo espaçamento uniforme de antenas. Quando os sinais de todas as antenas estão sincronizados em fase na direção do sinal desejado, ocorre uma interferência construtiva na direção desejada e destrutiva em outras direções (Mucci, 1984).

O *beamforming* adaptativo, em contraposição ao método tradicional, ajusta dinamicamente os pesos das antenas com os subsídios fornecidos pela matriz de covariância. Essa capacidade habilita esse método como sendo o mais confiável e eficaz em ambientes complexos, com interferências e DOA do sinal de interesse variáveis (Sallomi; Ahmed, 2015). A Figura 2 mostra o diagrama simplificado de um *beamforming* adaptativo, em que os algoritmos são empregados para calcular e otimizar os pesos das antenas em tempo real, de forma a maximizar o sinal desejado e minimizar interferências. Pelo esquema simplificado, nota-se que ocorre uma filtragem adaptativa, na qual a diferença entre o sinal de saída y(n) e o sinal de referência d(n) resulta no erro e(n), que é objeto de minimização por parte dos algoritmos adaptativos *(Melvin; Scheer, 2013).*

Este trabalho restringiu-se ao estudo dos algoritmos que foram efetivamente aplicados nas simulações, a saber, *Minimum Power Distortionless Response* (MVDR) e *Linearly Constrained Minimum Variance* (LCMV). Algumas aplicações podem ser afetadas pela rígida restrição imposta pelo MVDR, que é considerado por Manolakis, Ingle e Kogon (2005) um beamformer ótimo. Van Trees (2002) acrescenta que o principal problema de um caso ideal é a sensibilidade entre o ambiente de propagação e as condições impostas na concepção da formação ótima de feixes. Essa preocupação decorre da possibilidade de supressão do próprio sinal desejado em caso de imprecisões nas estimativas da DOA, o que sugere uma inadequação à tarefa de operar em ambientes complexos como o aéreo.

Figura 2: *Beamforming* adaptativo: esquema simplificado



Fonte: Autoria própria (2023)

No entanto, é possível aplicar condicionantes apropriadamente projetadas que, embora correspondam a um padrão inferior ao ótimo, não afetam a Signal-to-interference-plus-noise ratio (SINR) de forma relevante e atendem aos propósitos de minimizar os sinais indesejáveis e torná-los diferenciáveis dos sinais de interesse. Esse algoritmo que possui flexibilidade na quantidade e no grau das restrições é o LCMV e que, por essas razões, é considerado uma versão generalizada do MVDR.

Diante dos fatores mencionados, é compreensível pressupor uma relação estreita entre arranjo de antenas, matriz de covariância e o tipo de *beamforming adotado*. Portanto, percebe-se a necessidade de explorar os principais aspectos e princípios de funcionamento que constam do escopo da formação de feixes. O Quadro 2 fornece os principais fatores a serem considerados na implementação de um sistema anti-*jamming* em receptores ADS-B uilizando a técnica de *beamforming*.

Quadro 2 : Considerações gerais sobre a implementação de um sistema anti-*jamming*

Campo	Descrição
Arranjo de Antenas	Estruturas planares possuem a capacidade de distinguir objetos em azimute e em elevação, o que os credencia para operação em ambientes dinâmicos (Balanis, 2016). Opta-se pelo arranjo retangular em relação ao circular pelo melhor desempenho em elevação oferecido pelos Arranjos Retangulares Uniformes (URA).
Algoritmos de Estimação da DOA	No que concerne à adequabilidade em ambientes dinâmicos, Balanis (2016) considera os algoritmos ESPRIT (Estimação de Parâmetros de Sinal por Técnicas de Invariância Rotacional) e a evolução do MUSIC (Classificação de Múltiplos Sinais), denominado Root-MUSIC boas opções para emprego em ambientes complexos.
Algoritmos de Ajuste de Pesos das Antenas	Os algoritmos fazem parte do escopo do trabalho, com detalhes adicionais na seção seguinte. Eles são usados no *beamforming* adaptativo e devem ser eficazes em ambientes aéreos complexos como o aéreo.
Processamento de sinais	Há uma demanda para o uso de Processadores Digitais de Sinais (DSP) em sistemas anti-*jamming*. O DSP permite aproveitar amostras digitais, usando a matriz de covariância para estimar a Direção de Chegada (DOA) e ajustar os pesos das antenas com algoritmos específicos.

Fonte: Elaborado pelo autor (2023)

3 COMPARAÇÃO DOS RESULTADOS OBTIDOS

Anteriormente, foram realizadas discussões acerca do conceito de *beamforming* e da sua operacionalização por um sistema capaz de incorporar as valências necessárias à supressão de interferências. Nesta seção, são analisados os resultados das simulações, a fim de que seja determinado em que medida o emprego de técnicas de *beamforming* em receptores ADS-B sujeitos à Medidas de Ataque Eletrônico do tipo *jamming* seriam eficientes.

Os três ambientes operacionais que serão explorados são modelados em função de uma base de parâmetros comuns, acrescentados das particularidades impostas em cada caso de uso, que serão descritas nas subseções correspondentes. Para tanto, a Tabela 1 apresenta as variáveis que permanecem fixas durante toda a bateria de simulações.

Outro aspecto importante diz respeito ao escopo das simulações: em que pesem os papéis fundamentais dos algoritmos de DOA e da matriz de covariância no desempenho do *beamforming*, a modelagem do sistema se limita a subsidiar o estudo do comportamento dos algoritmos de formação de feixes propriamente ditos. Por esse motivo, a DOA é estipulada de forma arbitrária nos três cenários, sem prejuízos ao cumprimento dos objetivos deste trabalho.

Para tanto, a Tabela 1 apresenta as variáveis que permanecem fixas durante toda a bateria de simulações. Outro aspecto importante diz respeito ao escopo das simulações: em que pesem os papéis fundamentais dos algoritmos de DOA e da matriz de covariância no desempenho do *beamforming*, a modelagem do sistema se limita a subsidiar o estudo do comportamento dos algoritmos de formação de feixes propriamente ditos. Por esse motivo, a DOA é estipulada de forma arbitrária nos três cenários, sem prejuízos ao cumprimento dos objetivos deste trabalho.

Tabela 1 - Parâmetros fixos referentes às fases de simulações

Parâmetro	Descrição
Frequência da portadora	1090 MHz
Arranjo de antenas	URA [5x5]
Espaçamento entre elementos consecutivos	0,5 comprimento de onda
Frequência do pulso	18 KHz
Potência de transmissão do sinal desejado	500 W
Potência do ruído	0,5 W
Meio de propagação	Espaço livre

Fonte: Autoria própria (2023)

Adicionalmente, esta simulação não abrangeu a conversão Analógico-Digital (A/D) no receptor. Optou-se por não realizar a etapa de quantização no receptor modelado, de forma que haja a visualização dos resultados posteriores à aplicação das técnicas de *beamforming* no formato analógico. Assim, a conversão A/D é feita após a atuação dos algoritmos de *beamforming*. Se por um lado essa extrapolação não ocorre na prática, por outro fornece uma comparação entre o sinal analógico incidente no arranjo de antenas e o sinal digital, ambos em momentos subsequentes à atuação das técnicas de *beamforming*.

O presente trabalho realizou a análise do desempenho dos algoritmos de *beamforming* na supressão de interferências em ambientes progressivamente complexos. O primeiro cenário emprega a técnica *Phase Shift* beamformer; o segundo utiliza o algoritmo MVDR; e o último analisa o desempenho do algoritmo LCMV em situações nas quais não é possível realizar a determinação precisa da DOA do sinal desejado.

O ambiente de simulação no software Simulink, diante de quaisquer particularidades, encontra-se apto a fornecer informações acerca do sinal desejado, em amarelo; do sinal obtido após o emprego das técnicas de *beamforming*, em azul; da capacidade de reconstrução do sinal pelo estabelecimento de um limiar de amplitude, também em azul, porém em formato digital; e da porcentagem de bits errados, pelos comandos do *software* MATLAB.

3.1 Primeiro caso: *Phase Shift* (PS)

Conforme visto anteriormente, sugere-se que um sistema de recepção ADS-B necessite de mecanismos capazes de incrementar a qualidade da reconstrução do sinal. Para tanto, recorre-se à técnica *Phase Shift* de *beamforming* convencional para emprego em um meio composto apenas pelo sinal desejado, pelo ruído térmico do receptor e por dois *jammings*. A Tabela 2 fornece os dados adicionais para esse cenário.

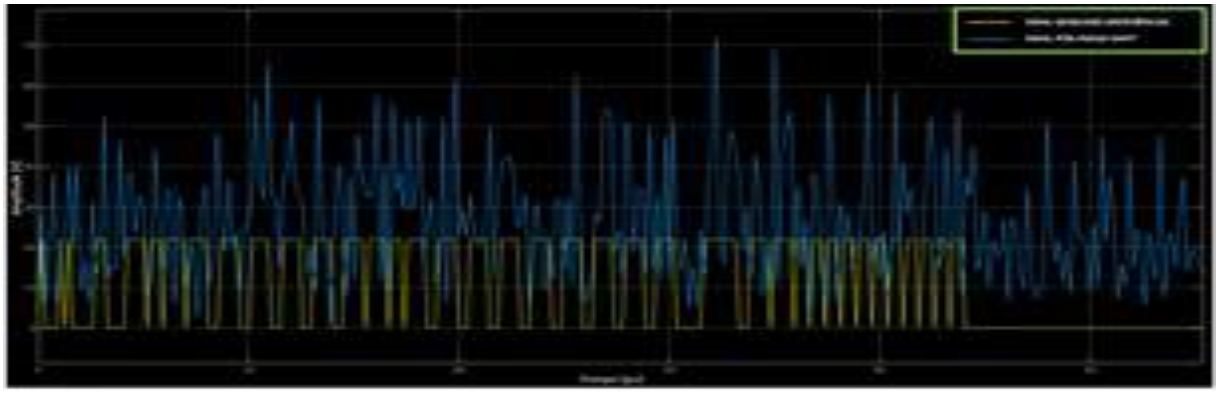
Tabela 2 - Parâmetros adicionais para o cenário "sinal desejado + ruído+*jamming*"

Parâmetro	**DOA**
Sinal desejado	45° em azimute e 10° em elevação
Estimativa do sinal	45° em azimute e 10° em elevação
Jamming	*Jammer* 1: 30° em azimute e 10° em elevação
	Jammer 2: 50° em azimute e 20° em elevação
Potência do *jamming*	*Jammer* 1: 1 KW
	Jammer 2: 1 KW

Fonte: Autoria própria (2023)

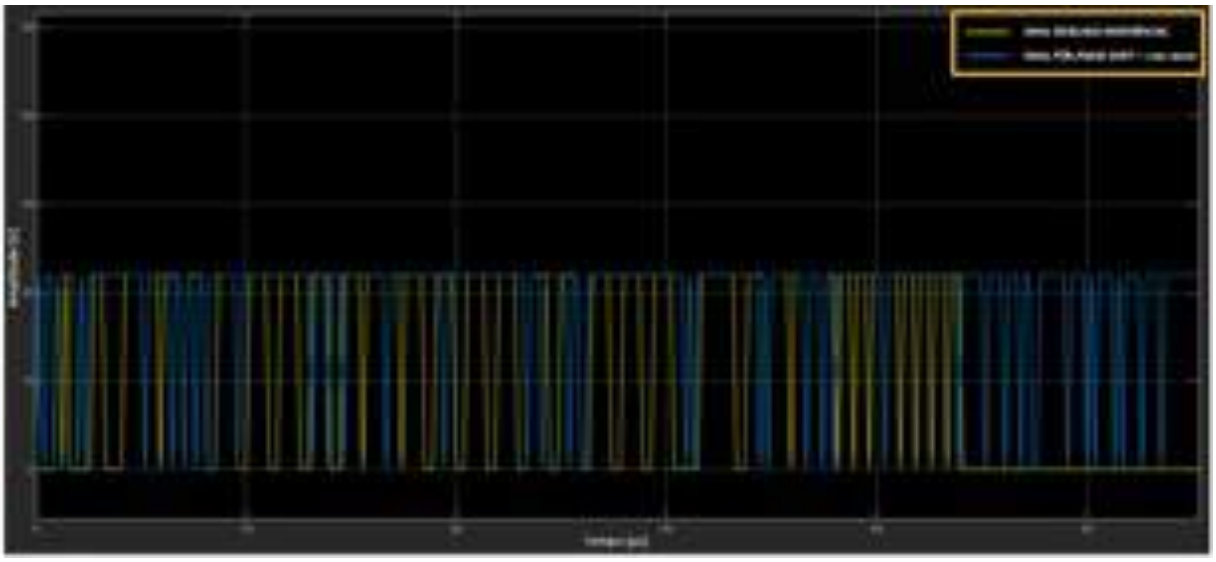
A técnica *Phase Shift*, em casos de maior complexidade, apresentam queda considerável na capacidade de recuperar a mensagem original. A introdução de dois *jamming*s degradam o sinal em grandes proporções, como se observa pelas Figuras 3 e 4. A taxa de bits errados aumenta para 43,04%, apontando para um caso de saturação.

Figura 3: Sinal desejado x Sinal após "PS" ("sinal desejado + ruído + *jamming*")



Fonte: Elaborado pelo autor (2023)

Figura 4: Sinal desejado x Sinal após "PS" ("sinal desejado + ruído + *jamming*") com limiar



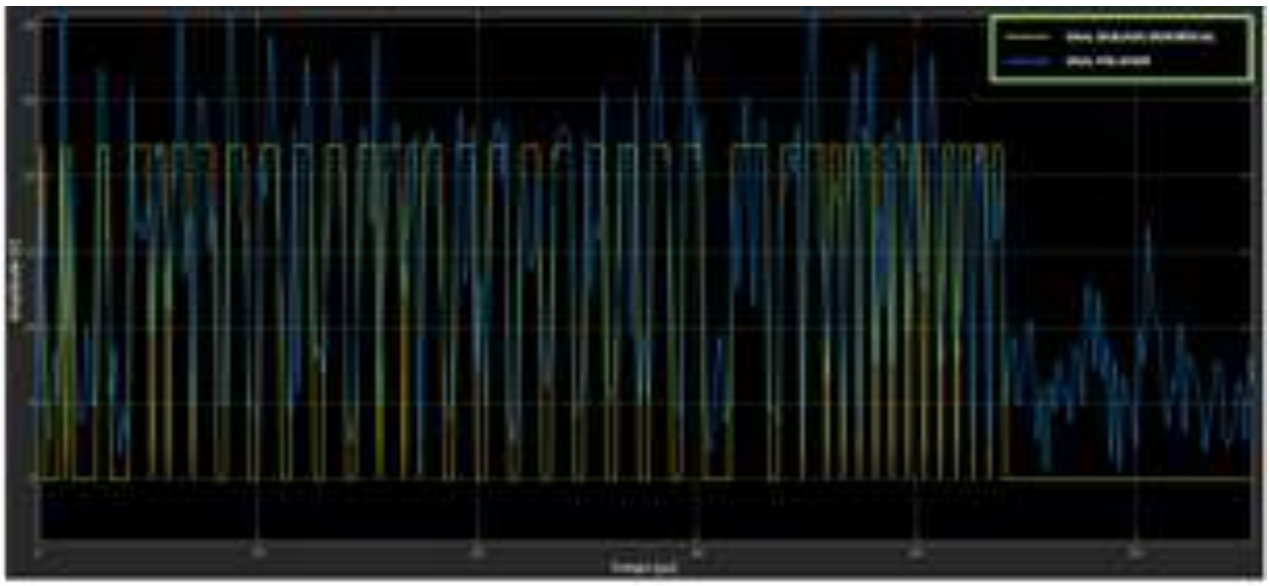
Fonte: Elaborado pelo autor (2023)

De modo a incrementar a complexidade dos ambientes operacionais de maneira apropriada, faz-se necessário atribuir a outros algoritmos a responsabilidade na contraposição às interferências.

3.2 Segundo caso: MVDR

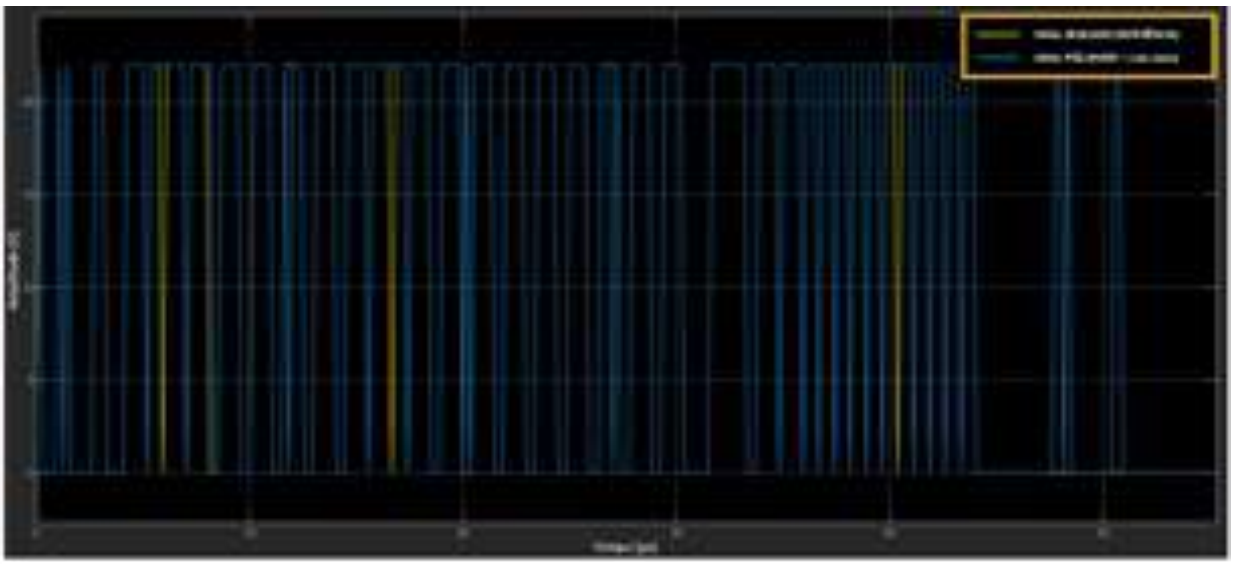
Nesse sentido, com o intuito de sobrepujar interferências pela tentativa de supressão desses sinais e da preservação do sinal de interesse, recorre-se ao algoritmo adaptativo MVDR. Utilizando-o em detrimento da *Phase Shift* beamformer e mantendo as condições impostas pela Tabela 2, são obtidos resultados significativamente melhores com relação à reconstrução do sinal, conforme se observa pelas Figuras 5 e 6.

Figura 5: Sinal desejado x Sinal após "MVDR" ("sinal desejado + ruído + *jamming*")



Fonte: Elaborado pelo autor (2023)

Figura 6: Sinal desejado x Sinal após "MVDR" ("sinal desejado + ruído + *jamming*")



Fonte: Elaborado pelo autor (2023)

Na Figura 6, é perceptível a capacidade do algoritmo possibilitar uma reconstrução do sinal incidente condizente com o desejado, com uma taxa calculada de bits errados a 3,56%.

Em contrapartida, em que pesem os expressivos resultados da qualidade de reconstrução do sinal desejado em meio às interferências, é preciso revisitar uma característica indesejada, inerente ao MVDR: conforme visto no capítulo anterior, por ser considerado um algoritmo ótimo de supressão de interferências, o MVDR necessita de uma estimativa precisa da DOA que, em termos práticos, pode ser afetada pela robustez do algoritmo de estimativa da DOA, pelo dispositivo DSP utilizado, pelas condições de propagação e, sobretudo, pela característica dinâmica conferida ao tráfego aéreo, com variações abruptas em altitude e em velocidade. Assim, diante dos conceitos apresentados, sugere-se que esse algoritmo não seja ideal para implementação em ambientes complexos, de forma que um eventual impacto decorrente de eventuais imprecisões é a supressão do próprio sinal desejado.

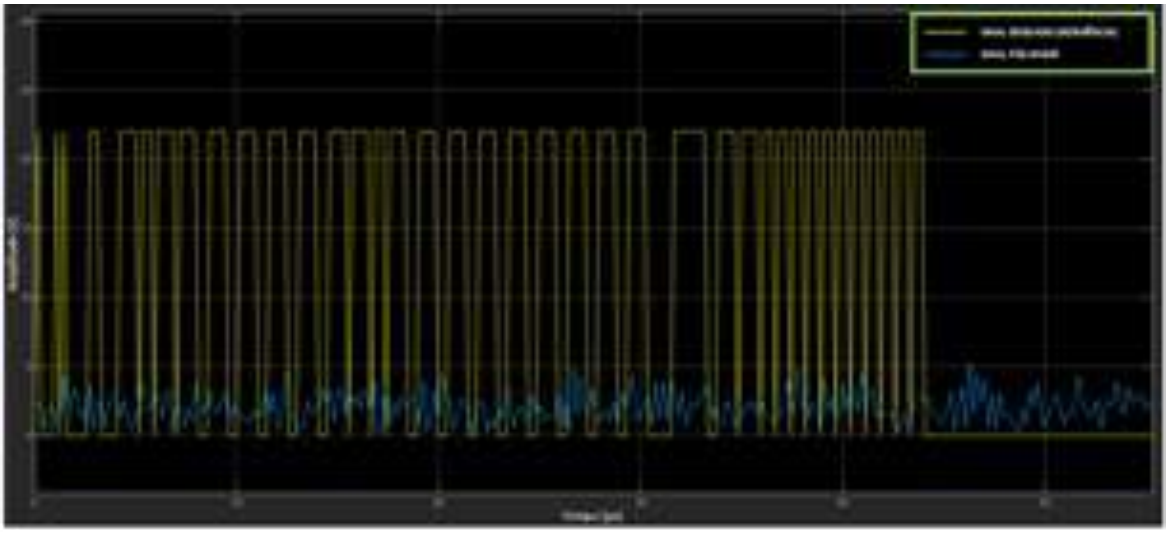
Diante do exposto, convém buscar a constatação dessas connsiderações em termos quantitativos. Para tanto, a Tabela 3 estipula os atributos utilizados nesse caso. Trata-se de uma simulação de ambientes complexos, em que há uma defasagem entre a DOA estimada e a DOA real do sinal desejado.

Tabela 3 - Parâmetros adicionais para o cenário "sinal desejado + ruído + *jamming* + imprecisões de estimativa da DOA"

Parâmetro	**DOA**
Sinal desejado	45° em azimute e 10° em elevação
Estimativa do sinal	43° em azimute e 10° em elevação
jamming	*Jammer* 1: 30° em azimute e 10° em elevação
	Jammer 2: 50° em azimute e 20° em elevação
Potência do *jamming*	*Jammer* 1: 1 KW
	Jammer 2: 1 KW

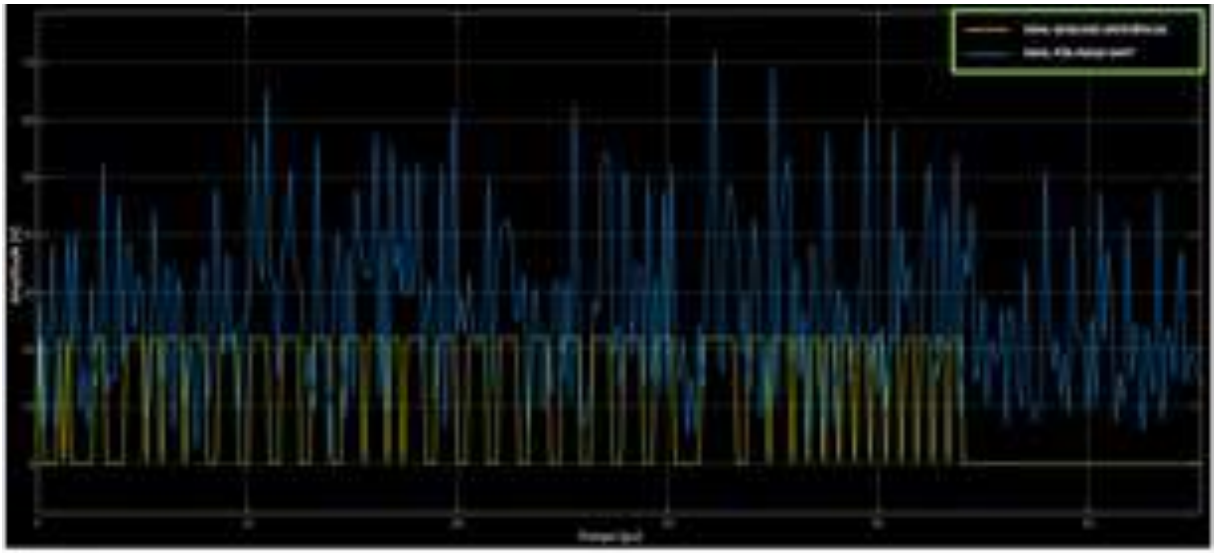
Fonte: Autoria própria (2023)

Figura 7: Sinal desejado x Sinal após "MVDR" ("sinal desejado + ruído + *jamming* + imprecisões de estimativa da D*OA*")



Fonte: Elaborado pelo autor (2023)

Figura 8: Sinal desejado x Sinal após "MVDR" ("sinal desejado + ruído + *jamming*+ imprecisões de estimativa da D*OA*") com limiar



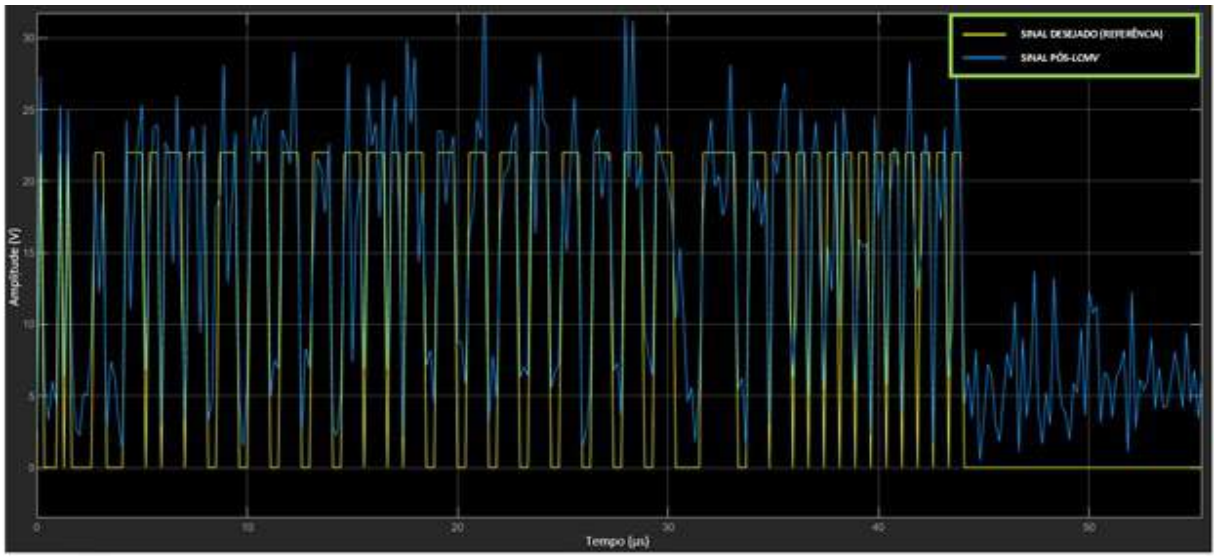
Fonte: Elaborado pelo autor (2023)

Dando prosseguimento ao raciocínio, na sequência é apresentado o algoritmo mais apropriado para lidar com ambientes operacionais complexos com a presença de *jamming* e estimativas imprecisas de DOA.

3.3 Terceiro caso: LCMV

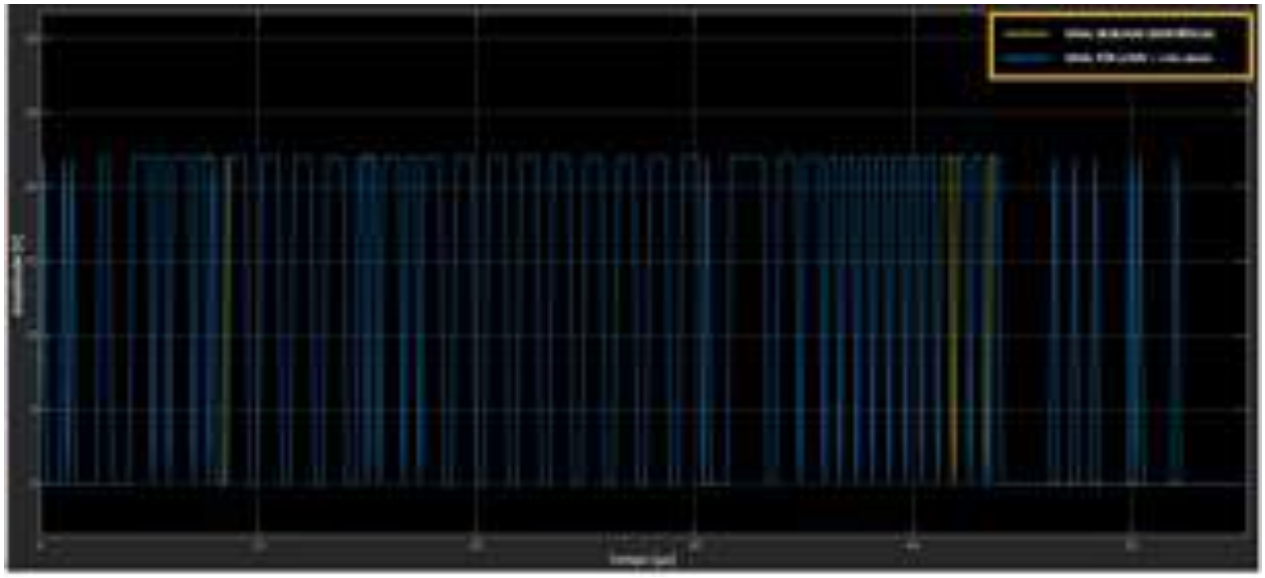
Identifica-se o algoritmo adaptativo LCMV como alternativa ao MVDR. Assim, é esperada a preservação do sinal em um intervalo maior de direções mediante o ajuste da matriz de restrições. As Figuras 9 e 10 exibem um padrão elevado de reconstrução do sinal, a uma taxa de bits errados de 3,6%. A Tabela 3 é utilizada como referência das condições adotadas nas simulações, ao passo que a matriz de restrições adotada nas simulações estipula o desvio da estimativa da DOA em ± 2º.

Figura 9: Sinal desejado x Sinal após "LCMV" ("sinal desejado + ruído + *jamming* + imprecisões de estimativa da D*OA*")



Fonte: Elaborado pelo autor (2023)

Figura 10: Sinal desejado x Sinal após "LCMV" ("sinal desejado + ruído + *jamming* + imprecisões de estimativa da D*OA*") com limiar



Fonte: Elaborado pelo autor (2023)

É possível descrever, pela Tabela 4, as taxas de bits errados calculadas no decorrer das simulações:

Tabela 4: Compêndio de taxas de bits errados calculadas durante a pesquisa

Cenário	**Técnica / Algoritmo empregado**		
	Phase Shift	**MVDR**	**LCMV**
Com Interferências	**Saturação**	**3,56 %**	3,6 %
Com Interferências e DOA imprecisas	Saturação	**Anula-ção**	**3,6 %**

Fonte: Elaborado pelo autor (2023)

Os valores em negrito correspondem àqueles descritos no decorrer da seção. Outro aspecto relevante da tabela são os termos saturação e anulação. Conforme mencionado no decorrer da seção, a taxa de bits errados é um parâmetro importante, que merece cautela, cuja interpretação não deve se limitar ao aspecto numérico. A despeito dos valores, esse parâmetro pode indicar, em certas ocasiões, nenhuma informação que não seja a completa saturação ou anulação do sinal.

Um resultado importante reside na representatividade das taxas de bits errados: conforme apresentado por Strohmeier et al. (2014), uma mensagem ADS-B é considerada corrompida quando ela apresenta mais do que 5 bits errados, traduzidos para o percentual de 4,16 % ao considerarmos uma mensagem completa, composta de 120 bits. Assim, os resultados indicam que seja possível empregar algoritmos adaptativos capazes de mitigar o efeito de interferências no receptor. Nesse contexto, faz-se mister a compreensão da finalidade do sistema, do ambiente de propagação e dos algoritmos que podem ser aplicados.

Por fim, nota-se que o algoritmo adaptativo LCMV mantém certa regularidade frente à progressão de complexidade dos ambientes, o que não é observado nos demais métodos testados. Adicionalmente, o tráfego aéreo se dá em ambientes complexos, com a participação de meios notadamente dinâmicos. Por essas razões, o LCMV é o algoritmo melhor credenciado a proteger receptores ADS-B de MAE do tipo *jamming*.

5 CONCLUSÃO

Os receptores ADS-B podem ser impactados negativamente por medidas de ataque eletrônico que afetem a disponibilidade dos sinais. Nesse a presente pesquisa examinou conceitos e conduziu experimentos que pudessem fundamentar a resposta da questão central que orientou os trabalhos: em que medida o emprego de técnicas de *beamforming* em receptores ADS-B sujeitos à Medidas de Ataque Eletrônico do tipo *jamming* seriam eficientes?

Com ponto de partida da pesquisa, efetuou-se a contextualização da evolução do controle do tráfego aéreo, tendo sido verificado que o ADS-B é considerado o estandarte das iniciativas de modernização do sistema de gerenciamento de tráfego aéreo em nível global. A partir da exposição de seus princípios básicos de funcionamento, identificou-se que a vantagem da transmissão de dados em radiodifusão poderia se tornar um importante objeto de exploração maliciosa por agentes mal-intencionados. Em um conflito, ser surpreendido por ataques em decorrência de uma consciência situacional deficiente pode gerar resultados catastróficos, com perdas de material e pessoal, podendo influenciar decisivamente no resultado de uma operação militar. Dessa forma, foram discutidas soluções que pudessem mitigar os possíveis efeitos de ataques eletrônicos do tipo *jamming*.

A partir da compreensão do conceito de *beamforming,* deduziu-se que essa poderia ser uma opção factível, do ponto de vista da capacidade de operação em ambientes complexos e da simplicidade de implementação. Para tanto, optou-se por realizar um delineamento das especificações anti-*jamming*.

Os resultados das simulações fornecem indícios claros de que a técnica *Phase Shift,* do *beamforming* convencional, e o algoritmo de *beamforming* adaptativo MVDR não possuem abordagens apropriadas à operação em ambientes complexos, como o aéreo, para fins de mitigação de interferências em receptores ADS-B. A técnica convencional obteve indicações de saturação completa do sinal, ao passo que o MVDR realizou o cancelamento do *jamming* e do sinal desejado, apontando para uma forte atenuação ou anulação do sinal.

sinal desejado, apontando para uma forte atenuação ou anulação do sinal.

Por essas razões, a pesquisa obteve a seguinte resposta à questão central: há indícios de que o algoritmo de *beamforming* adaptativo LCMV seria eficiente contra medidas de ataque eletrônico do tipo *jamming* em receptores ADS-B*,* uma vez que seu emprego demonstrou ser a única estratégia robusta face à progressão de complexidade dos ambientes operacionais, e à manutenção do parâmetro de taxa de bits errados estatisticamente abaixo do nível correspondente à 4,16%.

Por ocasião da conclusão do presente trabalho, a expectativa é de que a análise realizada acerca do emprego de técnicas de *beamforming* possa contribuir para a mitigação de possíveis vulnerabilidades que afetem a disponibilidade do sinal.

REFERÊNCIAS BIBLIOGRÁFICAS

ABDULAZIZ, Abdulrazaq; YARO, Abdulmalik S.; ADAM, Ashraf A.; KABIR, Mahmoud T.; SALAU, Habeeb B. Optimum receiver for decoding Automatic Dependent Surveillance Broadcast (ADS-B) signals. **American Journal of Signal Processing**, [s. l.], v. 5, n. 2, p. 23-31, 2015.

AIREON. **The Executive Reference Guide to Space-Based ADS-B**. McLean, Virgínia, 2023. 24 p. Disponível em: https://aireon.com/resources/brochures-guides/executive-reference-guide-space-based-ads-b/. Acesso em: 1 set. 2023.

BALANIS, Constantine A. **Antenna Theory:** Analysis and Design. 4. ed. Hoboken, Nova Jersey: John Wiley & Sons, 2016. 1104 p.

BALASEM, S. S.; TIONG, S. K.; KOH, S. P. *beamforming* Algorithms Technique by Using MVDR and LCMV. **World Applied Programming**, [s. l.], v. 2, 5. ed. p. 315-324, maio 2012.

CERQUEIRA, Raul Sandoval. Regulação para o ADS-B no espaço aéreo brasileiro. **Revista da UNIFA**, Rio de Janeiro, v. 34, n. 2, p. 21-35, 28 dez. 2021.

COMANDO DA AERONÁUTICA - COMAER. Departamento de Controle do Espaço Aéreo - DECEA. **Circular de Informação Aeronáutica nº16, de 22 de maio de 2023**. Apresenta o planejamento para a operacionalização do ADS-B OUT no Espaço Aéreo Continental Brasileiro. Operacionalização do Sistema de Vigilância Dependente Automática por Radiodifusão (ADS-B) no Espaço Aéreo Continental Brasileiro. Brasília, 2023a. p. 1-8.

GALATI, Gaspare et al. Study of an integrated communication, navigation and surveillance satellite system for air traffic management. **Proceedings of International Radar Conference**, Beijing, China, p. 238-241, out. 2002.

KIM, Yoohwan; JO, Ju-Yeon; LEE, Sungchul. ADS-B vulnerabilities and a security solution with a timestamp. **IEEE Aerospace and Electronic Systems Magazine**, [s. l.], v. 32, ed. 11, p. 52 - 61, nov. 2017.

LEITE JUNIOR, Walmor Cristino. A Guerra Eletrônica na História Naval. **Revista Marítima Brasileira**, Rio de Janeiro, v. 141, n. 1/3, p. 198-206, jan./mar. 2021.

MANESH, Mohsen Riahi; KAABOUCH, Naima. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. **International Journal of Critical Infrastructure Protection**, [s. l.], v. 19, p. 1-37, oct. 2017.

MANOLAKIS, Dimitris G.; INGLE, Vinay K.; KOGON, Stephen M. **Statistical and Adaptive Signal Processing:** Spectral Estimation, Signal Modeling, Adaptive Filtering and Array Processing. 2. ed. Norwood, Massachusetts: Artech House, 2005. 796 p.

MCCALLIE, Donald; BUTTS, Jonathan; MILLS, Robert. Security analysis of the ADS-B implementation in the next generation air transportation system. I**nternational Journal of Critical Infrastructure Protection**, [s. l.], v. 4, ed. 2, p. 78-87, ago. 2011.

MELVIN, William L.; SCHEER, James A. **Principles of Modern Radar**: Advanced techniques (Radar, Sonar and Navigation). Edison, New Jersey: Scitech Publishing, 2013. v. 2. 872 p.

MUCCI, Ronald A. A comparison of efficient *beamforming* algorithms. **IEEE Transactions on Acoustics, Speech, and Signal Processing**, [s. l.], v. 32, ed. 3, p. 548 - 558, jun. 1984.

SALLOMI, Adheed H.; AHMED, Sulaiman. Elman Recurrent Neural Network Application in Adaptive *beamforming* of Smart Antenna System. **International Journal of Computer Applications**, [s. l.], v. 129, n. 11, p. 38-43, 2015.

STROHMEIER, Martin et al. On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. **IEEE Communications Surveys & Tutorials**, [s. l.], v. 17, n. 2, p. 1066 - 1087, out. 2014.

UNITED STATES OF AMERICA - USA. Department of Transportation. Federal Aviation Administration - FAA. ADS-B 101: What It Is, and What It Means to You. **FAA Safety Briefing**, Washington, DC, v. 56, n. 2, p. 10-12, mar./abr. 2017. Disponível em: https:// www.faa.gov/general/faa-safety-briefing-marchapril-2017. Acesso em: 16 ago. 2023.

UNITED STATES OF AMERICA - USA. Department of Transportation. Federal Aviation Administration - FAA. **NEXTGEN Annual Report**: A Report on the History, Current Status, and Future of National Airspace System Modernization. Washington, DC: Federal Aviation Administration - FAA, 2020. 155 p.

VAN TREES, Harry L. **Optimum Array Processing:** part IV of Detection, Estimation, and Modulation Theory. Nova York: John Wiley & Sons, 2002. 1472 p.

Tática de Matilha 4.0: o emprego de veículos aéreos e de superfície não tripulados colaborativos em ações de ataque eletrônico

Primeiro-Tenente (MB) Christian **Toshio Ito**

RESUMO

O espectro eletromagnético (EEM) é um recurso crítico para a guerra naval moderna, utilizado para uma ampla variedade de tarefas essenciais, incluindo comando e controle (C2), comunicações, navegação e sistemas de guiagem de armas. Como resultado, as forças navais dependem cada vez mais da superioridade no EEM para operar em um ambiente cada vez mais complexo. Uma abordagem inovadora para garantir a superioridade no EEM é o emprego de Veículos Aéreos e de Superfície não Tripulados em ações de ataque eletrônico, operando de forma colaborativa e autônoma. O presente artigo apresenta uma análise sobre a aplicação da tática de matilha em ações de MAE, especificamente o bloqueio e despistamento eletrônicos, no ambiente operacional marítimo. Conforme o conceito de veículos não tripulados colaborativos, as vantagens proporcionadas pela cooperação entre estes sistemas potencializam o sucesso das operações em cenários complexos e hostis, especialmente se aplicados à guerra eletrônica. Os resultados obtidos por esse estudo apontam para a efetividade da tática de matilha em ações de ataque eletrônico, contribuindo para aprimorar as estratégias navais e a segurança em operações militares. Com base nessas conclusões, novas abordagens podem ser desenvolvidas para otimizar o uso colaborativo de veículos aéreos e de superfície não tripulados em operações futuras.

Palavras-chave: Veículos não tripulados. Tática de matilha. Ataque Eletrônico.

***Pack tactic*:** *The use of collaborative unmanned aerial and surface vehicles in electronic attack actions*

ABSTRACT

The electromagnetic spectrum (EMS) is a critical resource for modern naval warfare. The EMS is utilized for a wide array of essential tasks, including command and control (C2), communications, navigation, and weapon guidance systems. As a result, naval forces increasingly rely on the EMS to operate in an ever-growing complex environment. A novel approach to ensuring EMS superiority is the deployment of Unmanned Aerial and Surface Vehicles in electronic attack actions. This paper presents an analysis of the application of swarm tactics in electronic attack operations in the maritime operational environment. The central focus of the study lies in the application of swarm tactics for electronic attack operations, specifically addressing electronic jamming and deception in naval warfare. In line with the concept of collaborative unmanned vehicles, the advantages offered by cooperation among these systems enhance the success of operations in complex and hostile scenarios, especially when applied to electronic warfare. The findings from this study indicate the effectiveness of swarm tactics in electronic attack operations, aiding in refining naval strategies and enhancing security in military operations. Based on these conclusions, new strategies can be developed to optimize the use of collaborative unmanned aerial and surface vehicles in future operations.

Keywords: *Unmanned Vehicles. Wolfpack tactics. Electronic Attack.*

1 INTRODUÇÃO

O espectro eletromagnético (EEM) é um recurso crítico para a guerra naval moderna. O EEM é usado para uma ampla variedade de tarefas essenciais, incluindo comando e controle (C2), comunicações, navegação e sistemas de guiagem de armas. Como resultado, as forças navais dependem cada vez mais do EEM para operar em um ambiente cada vez mais complexo. A crescente dependência do EEM as torna vulneráveis a ataques de guerra eletrônica (GE). As ações de Medidas de Ataque Eletrônico (MAE) podem ser usadas para interromper as comunicações inimigas, bloquear seus radares e impedir o uso de armas com guiagem ativa por radar. Assim como podem ser usados para proteger forças navais amigas, ludibriando o oponente com táticas de dissimulação.

Para operar efetivamente no EEM moderno, as forças militares devem alcançar a superioridade do espectro eletromagnético (SRIVASTAVA, 2021). Contudo, meios navais e aeronavais convencionais com capacidade de ou dedicados à guerra eletrônica possuem elevados custos de aquisição e operação, e em situações táticas mais complexas acabam por expor suas tripulações a situações de risco. As recentes inovações tecnológicas na área de veículos aéreos e de superfície não tripulados constituem uma mudança de paradigma e um ponto de inflexão para o desenvolvimento de novas táticas que explorem seu potencial. Os modernos veículos aéreos e de superfície não tripulados possuem o grande potencial de operarem de maneira colaborativa em conjunto, ou não, com meios convencionais, podendo adotar uma nova forma de tática de matilha para executar missões de ataque eletrônico contra uma força naval oponente de capacidade bélica superior (LIU, 2019). Desta forma, a superioridade no espectro eletromagnético alcançada por meio do emprego desses veículos, por meio da tática de matilha, pode servir como forma de desafiar assimetricamente uma força hostil que possui a vantagem em termos de poderio bélico.

Através de revisão bibliográfica de literatura especializada, o presente trabalho explora o emprego dos veículos aéreos não tripulados (VANT) e veículos de superfície não tripulados (VSNT), especificamente em ações de ataque eletrônico, utilizando uma nova forma de tática de matilha, a fim de assegurar a superioridade no espectro eletromagnético e assim permitir a neutralização da força naval hostil em um ambiente operacional complexo e assimétrico.

2 A TÁTICA DE MATILHA E OS VEÍCULOS NÃO TRIPULADOS COLABORATIVOS

Com os avanços tecnológicos nas áreas de veículos não tripulados, inteligência artificial e sensores embarcados, o emprego tático desses meios está em constante evolução. Antes operados como mera extensão dos sensores dos meios navais e aeronavais e em tarefas de menor complexidade, a tendência é que esses veículos operem de forma autônoma e em conjunto com navios e aeronaves tripuladas, ou até mesmo sem a presença destes.

Uma abordagem não convencional para o emprego desses veículos em ações de MAE é operá-los em uma tática de matilha. Ao combinar VANT e VSNT no contexto das operações multidomínio, será possível estabelecer a superioridade no espectro eletromagnético em áreas extensas por longos períodos, com um custo operacional consideravelmente inferior se comparado ao emprego de meios tripulados. A variedade de sensores, bloqueadores e despistadores (*decoys*) eletrônicos embarcados em plataformas diversificadas possibilitará uma ampla gama de opções de ações de MAE em apoio às operações navais (Liu et al, 2019).

2.1 TÁTICA DE MATILHA

Ao observar o comportamento de certos predadores na natureza, uma forma de organização que promove a estrutura de caça baseada em ampla coordenação e comunicação entre os agentes é encontrada em animais como lobos e hienas, que são proeminentes nessa categoria, se organizando em unidades pequenas e móveis (matilhas). O sucesso dos predadores que utilizam táticas de matilha depende tanto de sua capacidade de se deslocar por períodos prolongados (permitindo a dispersão do grupo) quanto de sua organização e comunicações – que possibilitam a concentração coordenada no momento crítico da caça. O melhor exemplo de aplicação militar da tática de matilha é, sem dúvida, a campanha dos submarinos alemães *U-boat* na Segunda Guerra Mundial durante a Batalha do Atlântico (Arquilla, 2005).

O cerne da tática de matilha repousa em alguns elementos fundamentais. Em primeiro lugar, a coordenação efetiva entre unidades é essencial. A capacidade de responder a comandos de maneira rápida e precisa é crucial para o sucesso da tática. Qualquer desvio na execução do plano pode ter consequências significativas. Além disso, a flexibilidade tática é uma característica inerente à tática de matilha. As unidades devem ser capazes de se adaptar em tempo real às dinâmicas do campo de batalha e às ações do inimigo. Isso requer um alto nível de treinamento e confiança entre os membros da matilha.

A força da matilha também reside na complementariedade de habilidades. Cada unidade desempenha um papel único e contribui de maneira distinta para o objetivo comum. Seja por meio de habilidades ofensivas, defensivas ou de suporte, a diversidade de funções é crucial para o sucesso da tática.

A execução da tática de matilha passa por diversas fases. Inicialmente, há o planejamento estratégico, que envolve a definição detalhada do plano, a identificação de objetivos específicos e a atribuição de papéis para cada unidade. Em seguida, durante a movimentação em campo de batalha, a matilha se desloca de forma coordenada, mantendo comunicação constante entre as unidades. A fase de engajamento tático marca o contato com o inimigo. Neste momento, as unidades atuam de maneira sincronizada, empregando suas habilidades de forma combinada para superar as defesas adversárias e alcançar os objetivos estabelecidos previamente.

2.2 VEÍCULOS NÃO TRIPULADOS COLABORATIVOS

O conceito de veículos não tripulados colaborativos tem sido uma área de pesquisa e desenvolvimento em constante evolução no campo da engenharia e da tecnologia militar. Esses sistemas envolvem a coordenação e interação entre múltiplos veículos autônomos para alcançar objetivos comuns de forma sinérgica.

Detalhes técnicos envolvem a integração de tecnologias avançadas de inteligência artificial, sistemas de comunicações, sensores, processamento de dados em tempo real e capacidade de tomada de decisão autônoma. Esses elementos são fundamentais para permitir a colaboração entre os veículos não tripulados, possibilitando a troca de informações, a coordenação de tarefas e o ajuste de estratégias conforme as condições do ambiente operacional.

Na guerra moderna, os VANTs e VSNTs colaborativos têm sido aplicados em missões complexas e arriscadas, como reconhecimento em áreas hostis, ações de ataque coordenado em alvos estratégicos e operações de busca e salvamento. A utilização desses sistemas proporciona vantagens significativas, tais como a redução de riscos para os operadores humanos, o aumento da eficiência operacional e a capacidade de atuação em ambientes de difícil acesso ou perigosos.

De acordo com Feddema et al (2005), as perspectivas futuras para os veículos não tripulados colaborativos são promissoras, com o contínuo aprimoramento de suas capacidades técnicas e operacionais. Espera-se que esses sistemas se tornem ainda mais versáteis e integrados, permitindo uma colaboração mais sofisticada e efetiva entre diferentes tipos de veículos aéreos e de superfície. Além disso, a utilização de tecnologias de comunicação avançadas, como a rede 5G, poderá impulsionar a coordenação em tempo real entre os veículos, ampliando suas possibilidades de aplicação em contextos militares e não militares.

2.3 O EMPREGO DE VEÍCULOS NÃO TRIPULADOS EM TÁTICA DE MATILHA

A fusão da tática de matilha com veículos não tripulados colaborativos que empregam o conceito de inteligência de enxame representa uma convergência de estratégias militares e tecnologias avançadas que prometem transformar o paradigma operacional em cenários de conflito contemporâneos.
A essência desta abordagem reside na orquestração sinérgica de veículos não tripulados (VANT e VSNT) em uma rede altamente coordenada e interconectada. Esses veículos são dotados de algoritmos de aprendizado de máquina e sistemas de comunicações de última geração, permitindo a troca de informações em tempo real e a tomada de decisões autônomas em resposta aos estímulos do ambiente tático.

A coordenação avançada é alcançada por meio da implementação de protocolos de comunicação distribuída e algoritmos de roteamento eficientes. Essa rede colaborativa permite a disseminação de informações críticas de forma instantânea e sincronizada entre os veículos, possibilitando a resposta coordenada a eventos dinâmicos, como mudanças na posição do inimigo, o surgimento de novas ameaças ou a negação de sinais de posicionamento, navegação e tempo, como o GPS.

3 APLICAÇÃO EM AÇÕES DE MAE

Ao analisar o histórico do emprego da tática de matilha, observa-se que essa abordagem é particularmente favorável ao uso colaborativo de plataformas tripuladas e não tripuladas aplicadas em uma arquitetura de rede distribuída – onde podemos constatar a aplicação do conceito de guerra centrada em redes. Nesse contexto, a oportunidade de empregar essa nova tática na área de guerra eletrônica se destaca como uma alternativa que apresenta um custo-benefício atrativo e poderá se consagrar como um instrumento essencial para garantir a superioridade no espectro eletromagnético necessária à realização de operações multidomínio em um ambiente operacional marítimo contestado (Liu, 2019).

Propõe-se, assim, o emprego de veículos de superfície e aéreos não tripulados como plataformas para realizar ações coordenadas de guerra eletrônica, em uma área de operações vasta e por um longo período, em substituição a numerosos meios de superfície e aeronavais tripulados com um custo operacional superior e, principalmente, pondo em risco a segurança das tripulações, no caso de um conflito de alta intensidade. O emprego desses veículos seria opcionalmente coordenado por um navio de superfície com capacidades de GE, atuando como estação de controle das plataformas não tripuladas.

.

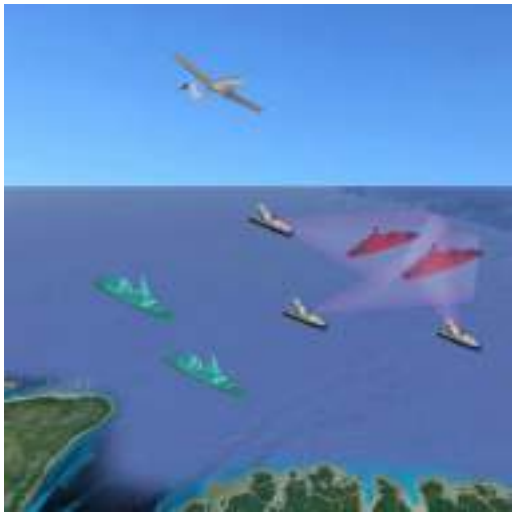
3.1 BLOQUEIO ELETRÔNICO

A tática de matilha de veículos não tripulados possui, em sua essência, uma aplicação de caráter ofensivo; desta forma, a principal tarefa a ser atribuída é a de bloqueio eletrônico (*jamming*). A tarefa de *jamming* poderá ser realizada tanto pelos veículos aéreos quanto os de superfície, e tal atribuição será decidida de acordo com a situação tática no momento da ação, podendo ser coordenada através de algoritmos de otimização.

De acordo com Neri (2018), como os veículos não tripulados possuem seção-reta radar (RCS) consideravelmente inferior às dos navios e aeronaves convencionais, eles poderão se deslocar na área de detecção dos radares inimigos com uma baixa probabilidade de serem detectados, onde poderão emitir um sinal de bloqueio próximo aos emissores, sendo necessária uma baixa potência para sua efetividade. Isto é particularmente útil, pois como são plataformas de dimensões reduzidas, a capacidade de geração de energia eletromagnética também será inferior, produzindo sinais de bloqueio de média e baixa potência.

Desta forma, a técnica de bloqueio proposta na tática de matilha é o bloqueio avançado (SFJ – *stand-forward jamming*). O SFJ será empregado para dar proteção aos meios navais e aeronavais que engajarão a força inimiga, onde a matilha de veículos não tripulados terá como área de operação o setor avançado em relação ao deslocamento da vaga atacante. Esta técnica permite a aproximação dos navios e aeronaves tripuladas para realizarem o ataque à força hostil com um reduzido risco de serem detectados pelos radares inimigos, conforme ilustrado na Figura 1.

Figura 1: VSNT em ação de bloqueio eletrônico contra navios hostis para mascarar a aproximação de navios amigos



Fonte: Elaborado pelo autor (2023)

Essa possibilidade de emprego é especialmente útil em um confronto entre forças com capacidades assimétricas. Neste caso, a superioridade no espectro eletromagnético, possibilitada pelo ataque eletrônico efetuado pela matilha de veículos não tripulados, será um fator de grande valor tático para opor-se assimetricamente a uma força naval com poder bélico superior, tendo em vista que a negação do amplo uso do EEM degradaria significativamente as capacidades da força hostil em manter a compilação do quadro tático.

5.2 DESPISTAMENTO ELETRÔNICO

Além das ações de bloqueio eletrônico, a "matilha" de veículos não tripulados também poderá empregar métodos de despistamento manipulativo (por meio de métodos de despistamento mecânico e eletrônico), a fim de gerar assinaturas eletromagnéticas falsas que induzam o inimigo ao erro, tanto em um contexto operacional focalizado – ao gerar uma compilação do quadro tático equivocada – quanto para um cenário amplo de dissimulação tática. A Figura 2 ilustra esse conceito.

Figura 2: VANT e VSNT utilizam a técnica de despistamento eletrônico para criar alvos falsos para enganar os radares de busca e vigilância do navio hostil.

Fonte: Elaborado pelo autor (2023)

Assim, o despistamento eletrônico poderá criar alvos falsos, iludindo o adversário quanto ao número de alvos em potencial que terá de enfrentar. Esses alvos falsos imitariam as emissões em radiofrequência (RF) e o RCS de plataformas reais, podendo também incluir chamarizes infravermelhos. Esse emprego tático do despistamento pode não apenas interromper as operações de um adversário, mas também, até certo ponto, ditar sua tomada de decisão no campo de batalha (TINGLEY, 2019).

Numerosos veículos não tripulados em tática de matilha podem cobrir extensas áreas geográficas, distribuindo as capacidades de GE de forma mais resiliente e descentralizada. Ao fazer isso, permite que a qualquer momento sejam criadas frotas de navios e aeronaves que não estão realmente presentes em uma área de interesse onde a força naval oponente possa estar operando, sendo uma formidável ferramenta de coleta de dados de inteligência quando se trata de sondar e avaliar as defesas do inimigo e registrar sua ordem de batalha eletrônica.

5 CONCLUSÃO

As evoluções tecnológicas na área da "Indústria 4.0" trazem, simultaneamente, novos desafios e oportunidades para a nossa Força Naval. As recentes mudanças geopolíticas apontam para um crescente ambiente de incertezas em nosso entorno estratégico, o que nos impele a considerar o emprego de novas tecnologias e a inovação no campo da tática, a fim de assegurar a nossa soberania no mar.

Dentre essas tecnologias se destaca o desenvolvimento de veículos aéreos e de superfície com capacidades de guerra eletrônica, que se operados de forma a explorar o seu pleno potencial podem ser valiosos multiplicadores de forças. Quando empregados em tarefas de ataque eletrônico podem garantir a superioridade no espectro eletromagnético, que é fundamental para a realização de operações multidomínio em um ambiente operacional complexo e contestado.

O pleno potencial dessas plataformas pode ser explorado se estas forem empregadas em uma tática de matilha, onde a diversidade de sensores e equipamentos de GE embarcados aliados à longa permanência e mobilidade na área de operações trazem uma considerável vantagem tática para a força naval.

Portanto, se aplicado em nosso cenário geoestratégico, o emprego de "matilhas" de veículos aéreos e de superfície não tripulados colaborativos em ações de MAE podem representar uma considerável vantagem tática em conflitos de alta intensidade

REFERÊNCIAS BIBLIOGRÁFICAS

ASSIS, O., et al. Dynamic orientation of receiver arrays using particles warm optimisation. **Eletronics Letters**, v. 49, n. 21, p. 1313-1315, nov. 2013.

ARQUILLA, J.; RONFELDT, D. **Swarming & The Future Of Conflict**. Disponível em: <https://www.rand.org/content/dam/rand/pubs/documentedbriefings/2005/randdb311.pdf>. Acesso em: 29 abr. 2023.

FEDDEMA, J. et al. **Military Airborne And Maritime Application For Cooperative Behaviors.** Disponível em:<https://www.osti.gov/servlets/purl/919642/>. Acesso em: 25 abr. 2023.

LIU, X. et al. **Application of unmanned surface vehicle in electronic warfare**. Disponível em: <http://www.kjdb.org/en/y2019/v37/i4/20>. Acesso em: 26 abr. 2023.

NERI, F. **Introduction to Electronic Defense Systems**. 3a Edição. Norwood, MA: Artech House, 2018.

SRIVASTAVA, S. **Electromagnetic spectrum – critical for military superiority.** Disponível em: <https://cenjows.in/wp content/uploads/2022/03/1.-electromagnetic-spectrum-ems-critical-for-militarysuperiority-by-lt-gen-sunil-srivastava_new.pdf>. Acesso em: 20 abr. 2023.

TINGLEY, B. **The navy's secretive and revolutionary program to project false fleets from drone swarms.** Disponível em: <https://www.thedrive.com/the-warzone/29505/the-navys-secretive-nemesiselectronicwarfare-capability-will-change-naval-combatforever>. Acesso em: 01 mai. 2023

VPN em redes privadas: criação de VPN para utilização em movimentos laterais

2º sgt (FAB) Huadson **Rudson** Araújo de Carvalho
2º sgt (FAB) **Ewerton** Mota dos Reis
3º sgt (FAB) **Nathália** Nascimento de **Souza**
3º sgt (FAB) **Kellen** Beatriz Ataide dos Santos

Acessar redes internas pode ser uma tarefa desafiadora devido a diversas medidas de segurança implementadas para proteger essas redes contra acesso não autorizado. Existem várias técnicas e ferramentas que podem ser utilizadas para tentar contornar essas medidas de segurança, dentre essas técnicas, a utilização de Virtual Private Network (VPN) se destaca como uma solução atrativa devido ao seu baixo custo, abordagem eficiente e versatilidade na exploração segura e anônima de redes.

A lateralização por VPN, também conhecida como VPN pivoting, consiste em utilizar uma conexão para redirecionar o tráfego de rede através de um servidor intermediário. Essa técnica oferece uma série de vantagens para os profissionais de segurança, pesquisadores e hackers éticos, ao permitir que explorem redes remotas sem comprometer sua identidade ou a segurança de seus dispositivos. (HAMMOUDEH, 2013)

A implantação da técnica pode ser facilitada pelo uso de contêineres. Esse recurso permite o compartilhamento e a implantação simplificada de imagens pré-configuradas, contendo as ferramentas necessárias para a exploração de redes. Essa abordagem aumenta a portabilidade das soluções de exploração e acelera o processo de configuração, tornando-a mais acessível e eficiente. (PIRES, 2020)

Outra possibilidade é sua aplicação em dispositivos móveis. Ao executar o servidor VPN em um dispositivo móvel, torna-se possível executar a técnica de VPN pivoting de maneira mais flexível, devido à facilidade de se transportar e conectar o dispositivo em redes wi-fi. Neste artigo, será explorado com maior profundidade algumas técnicas de lateralização utilizando VPN, suas aplicações práticas e suas limitações. Na prática, três técnicas de implementação da laterização com servidor VPN foram trabalhadas, sendo elas: com host debian, usando contêiner e também o uso de dispositivos móveis, conforme descrito nos apêndices A, B e C, respectivamente. A compreensão e domínio dessas técnicas podem fornecer uma base sólida para a exploração de redes privadas de forma simples, flexível e com boa performance.

A seguir, serão citados alguns casos onde podem ser aplicadas as técnicas de exploração usando VPN pivoting:

a) Pentest remoto em redes corporativas: permite que profissionais de segurança realizem testes de forma remota, explorando a infraestrutura de rede e avaliando a eficácia das medidas de segurança implementadas. Isso inclui a identificação de pontos fracos em firewalls, roteadores, servidores e outros dispositivos de rede, fornecendo insights para aprimorar a segurança e evitar possíveis ataques;

b) Pesquisa em segurança: pesquisadores de segurança e hackers éticos frequentemente utilizam este método para fins educacionais e de conscientização. Esses profissionais exploram ambientes controlados para descobrir e documentar vulnerabilidades em sistemas, aplicativos e dispositivos. Eles podem realizar análises aprofundadas em busca de falhas de segurança, que podem ser relatadas aos desenvolvedores ou fabricantes para que as correções adequadas sejam implementadas;

c) Testes de segurança em aplicativos web: o uso da VPN para movimentos laterais pode ser aplicada em testes de segurança de aplicativos web. Ao utilizer a técnica de tunelamento via VPN, os profissionais de segurança podem redirecionar o tráfego de um servidor intermediário para uma aplicação web em uma rede segregada, analisando as vulnerabilidades existentes, como injeções SQL, cross-site scripting e autenticação inadequada. Isso auxilia no fortalecimento da segurança das aplicações e na proteção dos dados dos usuários.

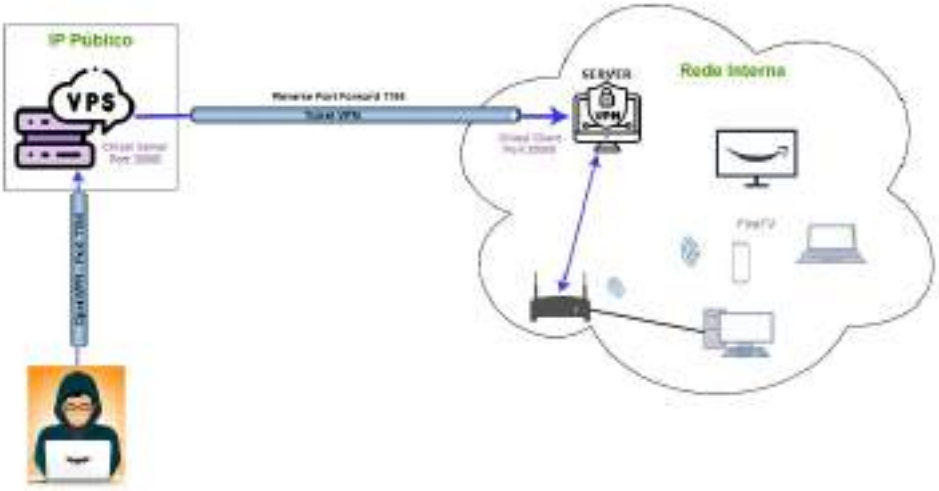
Para que essas atividades funcionem por lateralização, se faz necessário um conjunto de configurações que possibilitem o acesso à rede alvo.

Em uma situação ideal, o acesso a esses ambientes de teste poderiam ser fornecidos através de um serviço de VPN ou através de acesso físico no ambiente a ser testado.

Entretanto, caso não exista esse serviço disponível, um pentester pode levanter um ambiente de VPN próprio, diretamente na rede interna do ambiente a ser testado.

Na imagem abaixo, é possível visualizar como acontece o tráfego de dados para que a conexão entre o pentester e a rede interna a ser analisada seja feita através de um servidor VPN disponibilizado na rede local.

Figura 1 - Estrutura de funcionamento da lateralização por VPN.



Fonte: Autores (2023)

Para viabilizar o acesso a uma rede interna via necessário cumprir duas etapas, sendo elas: VPN conforme o cenário da imagem acima, é

Quadro 1 – Fases de criação do ambiente

Passo	Funcionamento
1	Criação do servidor VPN no dispositivo que servirá como ponto de acesso para a rede alvo;
2	Inicialização do chisel server em uma VPS;
3	Execução do chisel client no mesmo dispositivo do VPN server. Esse passo tem como objetivo criar um reverse port forwarding, utilizando a VPS como pivô, de modo a direcionar o tráfego que chegue na porta 1194 da VPS para a porta 1194 da máquina com o servidor VPN, que estará na rede interna.

Quadro 2 – Fases de conexão na VPN

Passo	Funcionamento
1	A máquina atacante solicita pela internet à VPS conexão VPN na porta 1194
2	A VPS por sua vez, recebe a solicitação na porta 1194 e através do túnel reverso criado pelo chisel, encaminha a requisição para a porta configurada para a estação com o VPN server na rede local;
3	O servidor VPN recebe a solicitação do cliente através do encaminhamento e retorna as informações para VPS através do encaminhamento do chisel;
4	Se estabelece uma conexão com o serviço na rede local. O pentester, então, pode se conectar aos dispositivos existentes na rede interna, através da VPN. O tráfego de dados é criptografado e transmitido de forma segura entre o cliente e o servidor VPN.

Fonte: Autores (2023)

Neste momento, o atacante tem acesso à rede onde está o servidor de VPN, podendo explorar toda ela como se localmente lá estivesse. Cabe ressaltar que essa transferência de dados ocorre de maneira criptografada, garantindo a confidencialidade das informações transmitidas. A utilização do redirecionamento de portas com chisel permite que o cliente acesse os serviços através da internet de forma transparente, como se estivesse conectado diretamente à rede do alvo. (Pillora, 2022)

Os passos de configuração citados podem ser automatizados, com fito de facilitar ainda mais sua implementação e acelerar a configuração, pra isso, o uso de contêineres pré-configurados, como os disponíveis no Docker Hub, simplificam e agilizam a implementação dos servidores de VPN bem como sua lateralização,

fornecendo uma distribuição padronizada de ferramentas e ambientes. Isso reduz o tempo e o esforço necessários para preparar o ambiente de exploração, permitindo que os profissionais de segurança se concentrem diretamente nas atividades de teste e análise. (Positivo Tecnologia, 2017)

Além disso, a facilidade de uso dos contêineres é um fator que torna essa prática mais acessível, em poucos comandos é possível controlar o ambiente de exploração, iniciando, parando e reiniciando os contêineres conforme necessário. Em síntese, a utilização de contêineres pré-configurados oferecem benefícios práticos, como simplificação da implementação, portabilidade, segurança aprimorada e uma experiência de uso mais intuitiva, sendo amplamente adotada na comunidade de segurança para otimizar o processo de exploração de redes.

Outra possibilidade de técnica, seria o uso de dispositivo móvel operando kernel linux com OpenVPN server. O fato de ser um dispositivo de tamanho físico reduzido torna-o mais discreto, facilitando a anonimização física durante as atividades de exploração. Essa estratégia possibilita que os profissionais de segurança realizem testes em redes wi-fi de maneira anônima, assegurando que suas atividades não despertem atenção indesejada.

Em suma, a utilização de um dispositivo portátil com um kernel Linux e servidor VPN oferece uma combinação de mobilidade, segurança e anonimato físico no contexto de exploração de redes através de um ponto de acesso wireless. Essa abordagem possibilita que profissionais de segurança realizem a exploração na rede de maneira eficiente, discreta e segura. (D'Aquino, 2014).

Para a criação do servidor VPN em dispositivos móveis, iremos utilizar o NetHunter, que consiste em uma plataforma de segurança cibernética baseada no sistema operacional Kali Linux, projetada para dispositivos móveis Android. Ela fornece ferramentas e recursos para pentest e avaliação de vulnerabilidades, permitindo executar ferramentas do Kali em um dispositivo Android.

Vale ressaltar que o NetHunter na sua versão completa, está disponível somente em alguns modelos de aparelhos específicos.

Do exposto, percebe-se que o pivoteamento via VPN pode ser realizado de diferentes formas, cada uma tendo suas particularidades.

A adoção de contêineres pré-configurados agilizam a implantação do ambiente, através da utilização de máquinas previamente configuradas.

A criação do ambiente utilizando dispositivos móveis pode ser um pouco mais complexa, porém, tem como vantagem a discrição física e a mobilidade, permitindo que os profissionais de segurança realizem testes de penetração em redes de forma discreta e eficiente.

Portanto, as técnicas de exploração de rede utilizando movimentos laterais por VPN, mencionadas e trabalhadas neste projeto, podem proporcionar aos profissionais de segurança recursos para realizar análises e testes em redes de maneira remota, segura e eficaz.

Essas abordagens otimizam o processo de exploração, garantem a privacidade e a confidencialidade das informações, além de permitir que várias pessoas acessem o mesmo ambiente de testes, de maneira remota e sem a necessidade da criação de servidores de VPN da organização a ser testada.

REFERÊNCIAS BIBLIOGRÁFICAS

D'AQUINO, Fernando. Kali NetHunter: o software que transforma o Android em uma arma hacker. Tecmundo. 2014. Disponível em: https://www.tecmundo.com.br/ataque-hacker/63603-kali-nethunter-software-transforma-o-android-arma-hacker.htm. Acesso em: 19 maio 2023.

HAMMOUDEH, Ayman. VPN Pivoting. Infosec. 2013 Disponível em:https://www.fir3net.com/security/concepts-and-terminology-security/vpn-pivoting-explained.html. Acesso em: 23 maio 2023.

KALI. Documentação nethunter. Kali Nethunter. 2023. Disponível em: <https://www.kali.org/docs/nethunter/>. Acesso em: 23 maio 2023.