A mensagem

EXÉRCITO PORTUGAL

Boletim Informativo
Regimento de Transmissões

Edição 2025

SUMÁRIO

FICHA TÉCNICA

Edição/Propriedade
Regimento de Transmissões

Diretor
Cor Tm Coutinho dos Santos

Direção Técnica
Cap Tm Edgar Ruano
Alf RC Ricardo Sobral

Edição Gráfica
Furr RC Miguel Quádrio Silva

ISSN 3051-6609

Editorial

Na edição de 2025 da Revista "A Mensagem", ano em que a Arma de Transmissões e o seu Regimento comemoram, respetivamente, o 55º e o 60º aniversário, focamo-nos como é costume na partilha das atividades da Arma, que decorreram ao longo do último ano, mas também na partilha de informação e de conhecimento que reflita alguns dos avanços, desafios e lições aprendidas, no domínio das comunicações, da guerra eletrónica e da cibersegurança em operações militares. Temos assim a espectativa que os leitores encontrem, na leitura da edição deste ano, informação que considerem pertinente.

A revista "A Mensagem", mantém a sua estrutura tradicional, iniciando com a mensagem do Exmo. Major-General Diretor Honorário da Arma de Transmissões, a que se segue a entrevista realizada pelos Tirocinantes de Transmissões ao anterior Presidente do Conselho da Arma de Transmissões, Brigadeiro-General Rui Bettencourt. Segue-se um artigo que explora o potencial da criptografia quântica para garantir comunicações seguras em ambientes de ameaça elevada, destacando os avanços na distribuição de chaves quânticas e os desafios para a sua implementação prática. O próximo artigo analisa a adoção do modelo Zero Trust em redes militares, enfatizando a importância da sua implementação para qualquer organização que procure fortalecer a sua postura de segurança. No último artigo deste primeiro grupo é descrito como as redes táticas heterogéneas e as "Coalition Waveforms" facilitam a interoperabilidade entre forças aliadas, permitindo operações coordenadas em ambientes de MultiDomínio.

O grupo seguinte de artigos inicia-se com uma revisão abrangente das principais atividades ao longo de 2024, dados estatísticos da Arma e a Formação no Regimento de Transmissões (RTm). Seguem-se quatro artigos relacionados com o apoio de comunicações em Forças Nacionais Destacadas (FND): um artigo sobre o papel da J6 Branch nas missões de treino e assistência militar em Moçambique, destacando os esforços na procura das melhores soluções para os desafios das Comunicações e Sistemas de Informação (CSI) da EUMAM MOZ; um artigo no âmbito da EUTM-MOZ sobre a importância da Ciberdefesa, face à crescente sofisticação das ciberameaças no domínio do ciberespaço; um artigo que aborda os desafios e soluções implementadas no módulo de comunicações durante as operações na República Centro-Africana, com ênfase na resiliência das redes em ambientes austeros; o quarto artigo analisa as comunicações da 5.ª Força Nacional Destacada na Roménia, com foco na interoperabilidade e eficiência. O próximo artigo do grupo, analisa a evolução das táticas de guerra eletrónica no conflito ucraniano, destacando o seu impacto no campo de batalha e a sua importância para o sucesso das operações. A finalizar este grupo um artigo sobre os desafios do aprontamento e projeção do PelCC 1FND/SVK.

Os últimos artigos, são como é hábito da autoria dos Alferes-Alunos Tirocinantes da Arma de Transmissões, abordando este ano temas bastante atuais e de elevada pertinência, nomeadamente relacionados com a Cibersegurança, a Inteligência Artificial, os Veículos não Tripulados, as Energias Renováveis, o Comportamento de Enxame e estratégias de Jamming e Spoofing.

Os temas abordados nesta edição refletem a crescente interdependência entre tecnologia, estratégia e operações militares. Desde a segurança quântica até à Guerra Eletrónica, os desafios do presente exigem inovação contínua no seio das Forças Armadas. Esperamos que esta publicação inspire novas ideias que ajudem a Arma de Transmissões a ultrapassar os seus desafios e que possam contribuir para o fortalecimento das capacidades militares do Exército.

Quero também destacar três acontecimentos marcantes ao longo do último ano: a inauguração da nova Caserna Modelo no RTm, um espaço moderno e funcional que permitiu modernizar as infraestruturas do RTm, levando a uma melhoria significativa das condições de alojamento e do conforto das Praças que pernoitam no RTm, o que reflete o compromisso do Exército Português com a excelência e a modernização das infraestruturas, servindo como exemplo da inovação que tem ocorrido no Exército nos últimos anos; a apresentação dos primeiros Praças do QP, estes militares estão habilitados com curso de formação, conferente da qualificação de nível 4, constituindo uma significativa mais valia para a Arma. Damos-lhe as boas vindas e reiteramos o nosso compromisso em continuar a desenvolver as suas capacidades e os valores militares que nos guiam; por fim destaco as atividades no âmbito do aprontamento da SigCoy do European Union Battlegroup 25-2/26-1, onde os nossos militares têm demonstrado mais uma vez um notável profissionalismo e a sua capacidade de adaptação a novos cenários.

A finalizar, agradecemos aos autores e colaboradores por partilharem os seus conhecimentos e experiências, sem eles não teria sido possível esta publicação. Uma palavra também de agradecimento a todos aqueles que participaram na edição e produção da revista.

Em 2025, continuamos a enfrentar um cenário global complexo, onde a tecnologia, a cibersegurança e a interoperabilidade desempenham papéis cruciais nas operações militares. Convidamos os leitores a refletirem sobre os temas apresentados e a participarem ativamente no debate sobre os desafios da Arma de Transmissões. Que continuemos a avançar juntos, com determinação e orgulho, em prol da Arma de Transmissões e do Exército Português.

Boa leitura!

O Comandante do Regimento de Transmissões,

Pedro Santos
Cor Tm

MENSAGEM DO DIRETOR HONORÁRIO DA ARMA DE TRANSMISSÕES

Major-General Viegas Pires

Com a publicação de mais uma edição da revista “A Mensagem”, o Boletim Informativo do Regimento de Transmissões, assinalamos simultaneamente o 55º aniversário da Arma de Transmissões e o 60º aniversário desta nobre Unidade do Exército.

O primeiro Regimento de Transmissões, “Regimento de Telegrafistas", surgiu em Lisboa, em 1926. Contudo, teve uma existência efémera, tendo sido extinto um ano depois, em 1927.

Só em 1965 voltou a haver um Regimento de Transmissões, desta vez no Porto, no quartel do Bom Pastor, com caráter permanente. Este regimento viria a deslocar-se para Lisboa, para o quartel de Sapadores, em 1977, onde se manteve até 2013, ano em que regressou ao Porto, para o quartel do Viso, onde hoje se encontra. Ao longo da sua existência teve diferentes missões, quer no âmbito das comunicações operacionais, quer no âmbito das comunicações táticas, bem como da guerra eletrónica e da ciberdefesa e, ainda, no âmbito do apoio à formação. Foram assim, 60 anos intensos e marcantes para as Transmissões do Exército, durante os quais o Regimento de Transmissões sempre soube responder com prontidão, eficiência e eficácia aos desafios que lhe foram colocados.

A criação do Regimento de Transmissões é anterior à criação da Arma de Transmissões. Apesar do emprego das Transmissões ser milenar, desde o uso de sinais sonoros e visuais, mensageiros apeados e a cavalo, pombos correios, até à utilização dos modernos meios de comunicação filares e sem fio, como o recurso a comunicações satélite, só em 1970 é que surgiu a Arma de Transmissões, no Exército português.

Apesar dos seus 55 anos de existência formal, como Arma, as Transmissões já mantinham estruturas efetivas no Exército, desde 1810, data da criação do primeiro Corpo Telegráfico, constituído por altura das guerras peninsulares e considerado a primeira unidade de transmissões do Exército.

Podemos dizer que a criação da Arma surge da necessidade de centralizar, num corpo especial independente, as valências e competências necessárias para fazer face a um incremento tecnológico que começava a ganhar dimensão e forma na década de 50 do século XX, um pouco impulsionado não só pelos avanços tecnológicos, mas também pela necessidade de responder aos desafios decorrentes dos compromissos então assumidos por Portugal, aquando da adesão à NATO, em 1949.

Aquando da sua criação, a Arma nasce no seio da Engenharia Militar e ganha a sua autonomia com as valências de comunicações permanentes e táticas, guerra eletrónica, manutenção e instrução, centrando a sua ação no apoio ao comando e controlo e no apoio de combate.

Atualmente, com uma guerra convencional, que se manteve por mais de três anos, em território europeu, tem sido patente a importância do comando e controlo, da guerra eletrónica, da superioridade da informação e do emprego crescente das ações de ciberdefesa. As Transmissões ganham assim, uma importância especial, nomeadamente quando voltamos a centrar a nossa preparação no âmbito da missão tradicional de defesa da OTAN (artigo 5º).

Uma saudação especial a todos os quadros e Tropas de Transmissões, que servem fora do território Nacional, com um profundo reconhecimento pela qualidade das funções que têm vindo a desempenhar, bem como às respetivas famílias, elementos essenciais para o efetivo sucesso de todos os que se encontram nessa situação.

Igualmente, saúdo os militares de Transmissões e civis que servem em território nacional, nas diversas unidades, estabelecimentos e órgãos do Exército, das Forças Armadas, em órgãos da administração direta e indireta do estado e na Presidência da República.

O Corpo Especial de Transmissões, que integra os praças, sargentos e oficiais de Transmissões do Exército, tem demonstrado, nas mais diversas situações, uma elevada aptidão, através esforço colocado na execução e concretização das tarefas e missões que lhe são atribuídas, imbuído de elevadas qualidades militares, com inovação, engenho e ciência, contribuindo para um Exército credível, moderno, atrativo, de elevada prontidão e competência.

Há assim, que aproveitar as oportunidades e potenciar as nossas capacidades, de modo a constituir o Corpo Especial de Transmissões como um instrumento ímpar ao serviço do Comandante do Exército, sempre pronto a enfrentar os desafios que nos sejam atribuídos, honrando o legado que nos foi transmitido por aqueles que antes de nós serviram neste Ramo das Forças Armadas e nas Transmissões,

Bem hajam!

O Diretor Honorário da Arma de Transmissões,
Nelson Martins Viegas Pires, MGen

Entrevista ao Exmo. Brigaderio-General Fernandes Bettencourt

Entrevista realizada pelos Oficiais Tirocinantes de Transmissões:
Alf Al Tm Tiago Silva;
Alf Al Tm SimãoNeves;
Alf Al Tm Younes Zidane;
Alf Al Tm João Silva;
Alf Al Tm Eduardo Esteves.

1. Meu General, que motivos o levaram a escolher a carreira militar, mais concretamente a Arma de Transmissões?

Em primeiro lugar aproveito para vos felicitar pelo vosso trabalho preparatório desta entrevista, e por vosso intermédio, a todo o corpo editorial da revista Mensagem por assegurarem a continuidade e a qualidade deste importante veículo de cultura e informação militar.

A minha opção em seguir a carreira militar está intimamente ligada com o ambiente em que cresci, filho de piloto aviador e inserido numa alargada e coesa família militar na Força Aérea.

A opção pelo Exército, e pela Arma de Transmissões, surgiu da conjugação de algumas situações concretas: a impossibilidade de ser piloto por uma inaptidão médica; a influência muito positiva que tive de instrutores e professores no Colégio Militar, designadamente do então Tenente-Coronel de Transmissões Bastos Moreira; o meu interesse pela eletrónica e pela programação, a década de 80 trouxe-nos as máquinas de calcular programáveis e os primeiros computadores acessíveis às famílias, como o *ZX Spectrum*; e a observação e aconselhamento já durante o período da Academia, em particular do Comandante do Batalhão de Alunos na Amadora, o então Major de Infantaria Comando Cunha Lopes. Tudo considerado, tornaram-na no final do 1.º ano a "óbvia" opção para o Cadete Aluno n.º 120, podendo hoje confirmar, 37 anos e uns meses mais tarde, ter sido igualmente a opção "correta".

2. Como vê o aumento de abates ao quadro de Oficiais e Sargentos de Transmissões e o que o Exército pode fazer para contrariar isto?

Com preocupação, em particular se olharmos ao passado recente, pois representam um número significativo para o nosso Quadro Especial, assumindo particular relevância por ser a Arma que, decorrente dos baixos ingressos na Academia Militar (AM) e na Escola de Sargentos do Exército (ESE), se encontra com maior pressão ao nível do rácio de existências face ao efetivo necessário, tendo sido identificadas e estando a ser tomadas medidas para procurar reforçar a atratividade e as entradas com destino à Arma.

Mas também apreensão, pois não obstante, as condicionantes pessoais, não raras vezes, terem motivações do foro interno ou de atração externa, observei que, ao longo do processo que leva à tomada de uma decisão tão disruptiva, existia uma deficiente comunicação e procura de aconselhamento junto de pessoas com maior experiência profissional.

No entanto, em resultado do empenho das chefias militares junto da tutela, das alterações já efetuadas e das propostas em estudo, penso que nos encontramos hoje em melhores condições para competir com a pressão externa.

O Exército, as Transmissões muito em particular, através da riqueza de funções e de projetos desafiantes disponíveis nos nossos diferentes domínios de intervenção, permitem assegurar o necessário equilíbrio entre as vertentes técnicas e a carreira militar. Os nossos militares têm a possibilidade de encontrar na Arma a realização profissional e pessoal que todos procuramos.

Quando, por exceção, tal deixa de acontecer, com o necessário conhecimento atempado pela cadeia de comando, será em muitas situações possível ajustar e corrigir as situações de insatisfação indo ao encontro dos comuns interesses do Exército e do militar, possibilitando-lhe o readquirir de motivação e condições para aplicar todo o seu conhecimento e experiência, melhor servindo assim o Exército e as Forças Armadas.

3. Como vê o papel das Transmissões nos conflitos contemporâneos e que ilações podemos retirar para o nosso Exército?

Na opinião isenta de alguém que é oriundo da Arma de Transmissões penso que, tal como com aqueles que nos antecederam no passado, o resultado da nossa ação materializa um fator decisivo para qualquer Força poder alcançar o sucesso na missão.

Esta opinião é sustentada não só na observação da importância dos sistemas de comunicação e Informação nos teatros de operações mais modernos mas, de forma mais singela, na centralidade e importância da nossa ação nos Exercícios que apoiamos, tal como provavelmente puderam observar durante os exercícios Leão da Academia. Sempre que algo corre mal num exercício, invariavelmente se encontrará que o "bode respiratório", como diria um conhecido treinador nacional, estará algures num qualquer sistema de informação ou meio de transmissão, seja rádio, filar ou mesmo mensageiro (não excluindo o pombo).

Passando a provocação, seja nos conflitos passados, como nos conflitos contemporâneos, o emprego de uma força militar num ambiente caracterizado pelo caos e pela desordem, tem por base a sua preparação prévia e assenta as condições de sucesso na arte de conseguir obter vantagem sobre um opositor nesse ambiente, através de uma ação concertada de esforços, designadamente da sincronizada e eficaz articulação entre as diferentes funções de combate.

A evolução tecnológica tem vindo a abrir novos domínios, trazendo para a esfera das operações militares o Espaço e o Ciberespaço, respetivamente o 4º e o 5º domínios de operações. Pretendo dizer com isto que o teatro de operações contemporâneo é forçosamente caracterizado por ser ambiente multidomínio, pois não será provável a existência de um conflito, mesmo que regional, que não envolva simultaneamente operações militares no espaço, no ciberespaço e pelo menos noutros dois, trazendo assim desafios e responsabilidades acrescidas para aqueles cuja missão é assegurar as condições para o sucesso da ação de Comando e Controlo do Comandante de uma Força, seja a que escalão for.

Conseguir operar a este nível comporta, naturalmente, um nível de complexidade elevadíssimo e ainda ao alcance de poucas nações, designadamente ao nível das ações de Comando e Controlo, mas o desenvolvimento de capacidades nestes domínios é incontornável.

Ao nível tático da Força Terrestre o sucesso da sua ação assenta no emprego sinérgico e coordenado de armas combinadas, pelo que a importância individual de cada uma das componentes da força é irrelevante. Não fará portanto sentido discutir quem terá menor ou maior relevância para o sucesso da missão. Certo é que sendo a sincronização e ação sinérgica a chave do sucesso, tal não se consegue sem o contributo da Arma de Transmissões. Quer na vertente do apoio em Comunicações e Sistemas de Informação, quer na componente de Guerra Eletrónica, quer na componente de Ciberdefesa.

Quanto às principais ilações a tirar, para lá da necessidade de nos mantermos atualizados e abertos a novas e inovadoras formas de ultrapassar os desafios no terreno, com leitura de relatórios e de outras publicações de referência referentes a estes conflitos, teremos forçosamente de reforçar o conhecimento e a proficiência no âmbito das atividades cibereletromagneticas, de ajustar as nossas Técnicas, Táticas e Procedimentos, e eventualmente, atendendo à imperiosa necessidade de dotar as Forças de maior capacidade de sobrevivência nos cada vez mais transparentes Teatro de Operações Contemporâneos, para poderem com rapidez e sem impacto na condução das operações, "dispersar para sobreviver, concentrar para combater", tendo este ponto particular impacto na missão dos futuros Nós de Acesso do Batalhão de Transmissões, com o eventual reforço de alguns dos seus equipamentos para melhorar o apoio CSI ao Posto de Comando de escalão Brigada ágil, flexível e dotado de maior capacidade de sobrevivência.

4. De todas as funções que desempenhou ao longo da sua carreira, qual foi a que mais o cativou e porquê? E qual o momento que o marcou mais significativamente ao longo da sua carreira?

Não consigo isolar numa única função, talvez nas desempenhadas em alguns períodos específicos, como enquanto Tenente e Capitão no projeto Redes Regimentais de Informação de Gestão (RRING), no extinto Centro de Informática do Exército (CIE), e já como Tenente-Coronel, na Direção de Comunicações e Sistemas de Informação (DCSI), como gestor do projeto para a criação, em parceria com a empresa Critical Software, do demonstrador de conceito do *Battlefield Management System* (BMS).

No CIE, onde desempenhei as funções de programador, de analista de sistemas, de gestor de bases de dados, e de chefe da secção de desenvolvimento de software da Repartição de Redes e Pequenos Sistemas, chefiada pelo então Tenente-Coronel de Transmissões José Canavilhas, vivi um período de enormes desafios pois o projeto RRING pretendeu proporcionar ao Exército um salto tecnológico significativo, com a criação de aplicações desenhadas especificamente para retirar partido das novas redes de dados e apoiar as unidades na digitalização dos seus processos. Para isso, tirámos partido do advento das redes locais, dos sistemas e tecnologias da Microsoft, com soluções cliente-servidor inovadoras, constituindo o Exército um dos primeiros Casos de Uso nacional para esta empresa.

No âmbito deste projeto preparou-se o futuro da arquitetura de serviços do Exército e implementou-se uma inovadora rede de dados com implantação em todo o território, continente e ilhas, com o Regimento de Transmissões (em Lisboa) a ter papel crucial na constituição das nossas redes metropolitanas e alargadas, missão herdada em 2014 pelo Centro de Transmissões do Exército (CTE) e que levou ao que hoje designamos de Rede de Dados do Exército.

Foi neste período que o Prémio Descartes do Instituto de Informática do Ministério das Finanças foi atribuído ao Exército, pela aplicação Recursos Financeiros para Windows (RFW) do RRING, momento que tornou visível ao Exército o real potencial e valor dos seus recursos internos, confirmando que estávamos na crista da onda nacional do desenho de arquiteturas tecnológicas e na produção de software de gestão, designadamente assente em tecnologias Microsoft.

Na DCSI, após regressar de Bruxelas, como chefe da Repartição de Sistemas para o Comando e Controlo, pela oportunidade que me foi dada pelo então Diretor Major-General Xavier Matias para coordenar os trabalhos da Equipa de Engenharia para o Projeto SIC-T, chefiada à data pelo Major de Transmissões Alberto Correia, e na qual assumi a gestão do projeto BMS para o Exército, dando continuidade ao recentemente estabelecido protocolo de cooperação técnica estabelecido entre o Exército e a *Critical Software*. Tive assim o privilégio de participar no nascimento desta capacidade no gabinete do comandante da Companhia de Transmissões da Brigada Mecanizada, comandada pelo então Capitão de Transmissões Vitor Custódio, literalmente a partir de um quadro em branco durante a primeira reunião técnica mantida com o gestor de projeto da empresa. Este sistema, que evoluiu ao longo de diversos estádios de investigação, permitiu o desenvolvimento de um protocolo de comunicações inovador para implementação por software de redes Mesh, que motivou a produção e apresentação de um paper no IEEE [*Institute of Electrical and Electronics Engineers*] e que se encontra presentemente instalado e em operação nas nossas unidades de manobra em Forças Nacionais Destacadas, constituindo hoje uma preciosa ferramenta de disponibilização da *Common Operacional Picture* (COP) em quase tempo real e permitindo a manutenção da *Situational Awareness* das Forças.

5. No âmbito das Transmissões, qual a área que considera que deveria ser reforçada quer ao nível de recursos materiais, quer ao nível de recursos humanos?

Embora reconhecendo que nunca temos o orçamento que gostaríamos de ter para proporcionar ao Exército as melhores soluções tecnológicas no âmbito das Comunicações e Sistemas de Informação, da Guerra Eletrónica, da Ciberdefesa e da Gestão da Informação e do Conhecimento, eu creio que ao nível dos materiais a principal questão se prende com o atraso na concretização de alguns dos nossos projetos estruturantes a nível tático, como é exemplo a componente de Comunicações do projeto SIC-T, atual projeto *Tatical Deployable Communications and Information Systems* (TDCIS). O Exército tem mantido uma forte aposta no investimento na capacidade Comando e Controlo Terrestre, mas o hiato entre a obtenção do financiamento e o lançamento de alguns concursos em conjuntura internacional muito adversa, mesmo não ambicionando ab initio adquirir "Ferraris", tem-nos forçado a ceder a compromissos para ajustar os objetivos à capacidade financeira disponível e às propostas comerciais apresentadas.

Não obstante, os tempos definitivamente mudaram, resultado do excelente trabalho desenvolvido nos últimos anos pelos nossos camaradas do Estado-Maior do Exército e pelos Gestores dos Projetos inscritos na Lei de Programação Militar (LPM), temos projetos estruturantes a entrar na sua fase de execução e concretização, como o Sistema de Combate do Soldado – C4I, que irá proporcionar um enorme salto tecnológico ao nível da função de combate manobra, trazendo modernos rádios de banda larga, de secção e pessoais, potenciando a disponibilização da COP até ao combatente apeado, através da utilização integrada dos nossos Sistemas de Informação para o Comando e Controlo (C2), como o *Dismounted Soldier System* - C2 e o BMS, colocando-nos na linha da frente dos exércitos modernos, bem como o já referido TDCIS, que, embora ainda necessite de reforço futuro em número de módulos para as necessidades do Exército para o estabelecimento da necessária infraestrutura tática CIS de suporte à Força Terrestre de Próxima Geração, trará no início do próximo ano o ambicionado salto tecnológico para as nossas comunicações táticas, e ainda o projeto *Cyber Defence* (CD) – *Deploy*, que mereceu prioridade para a sua concretização pelo Comando do Exército, e que se espera ser lançado a concurso muito em breve.

Acresce na infraestrutura CSI fixa, o forte investimento feito na capacidade de processamento no Centro de Sistemas Operacionais (CSO) do Exército, assente em nós de hiperconvergência, na capacidade de arquivo digital, na implementação do CSO Alternativo e, muito recentemente, em equipamento especificamente dedicado à utilização de tecnologias de Inteligência Artificial, designadamente para efetuar um piloto com o Estado-Maior do Exército com recurso a *Retreival Augmented Generation* (RAG) em *Large Language Model* (LLM) disponibilizado on-premises, de forma a capacitar a breve prazo as nossas FND, numa primeira fase ainda em apoio *Reach Back*, com a utilização destas ferramentas de forma segura.

Sim, o nosso Calcanhar de Aquiles tem estado na exiguidade dos nossos efetivos, face à necessidade de continuar a cumprir as nossas missões conjunturais, incluindo exercícios, empenhando os Elementos da Componente Operacional do Sistema de Forças, e igualmente estando sempre em operação ao nível da componente estrutural CSI do Exército nos Órgãos na dependência da DCI, Centro de Transmissões do Exército (CTE) e Centro de Guerra da Informação e Ciberespaço (CGIC), respetivamente no apoio CSI e na ciberdefesa.

Este é um constrangimento transversal a todo o Exército, mas assume maior relevância ao nível das Transmissões, quer na categoria de Oficiais como de Sargentos. A criação do Quadro Permanente da Categoria de Praças, em 2024, ajudou a mitigar um pouco a situação nesta categoria, como sabemos muito deficitária no Exército. O Comando do Exército está conhecedor da situação e a tomar medidas para colmatar a necessidade de graduados na Arma de Transmissões, estando a pugnar para melhorar a nossa atratividade, designadamente através da implementação de mecanismos para incremento das possibilidades de opção de ingresso, como sejam, no caso da categoria de sargentos, alargar o

ingresso direto na ESE a civis já habilitados com Curso Técnico Superior Profissional de Nível 5, e na categoria de oficiais na Academia Militar, com a avaliação de abertura à frequência de outras áreas científicas e tecnológicas no âmbito da engenharia.

6. Considera que a estrutura do curso de Transmissões da Academia Militar e do curso de Engenharia Eletrotécnica e de Computadores - Ramo Telecomunicações, do Instituto Superior Técnico, forneceram as ferramentas necessárias para o desempenho das suas funções ao longo da carreira?

Creio que a Academia Militar (AM) e o Instituto Superior Técnico me deram as ferramentas necessárias para o trabalho que eu realizei, principalmente na fase inicial da carreira. Aproveito para salientar neste aspeto a evolução a nível da preparação científica que a AM hoje vos assegura, substancialmente superior à do meu tempo, mas também não quero com isto dizer que não possam existir outras áreas do conhecimento que nos permitam adquirir ferramentas mais concretas noutros domínios com crescente relevância, como seja a área da ciência de dados. Temos no entanto de manter bem presente que, ingressando nos Quadros Permanentes das Forças Armadas, iniciamos um novo caminho de aprendizagem de saberes, seja pela riqueza de funções que temos oportunidade de desempenhar ao longo da carreira, com responsabilidade crescente no âmbito do comando e da liderança militar, bem como pela necessidade imperiosa de adquirir proficiência específica nas nossas áreas de responsabilidade das Transmissões ao nível da articulação e emprego de armas combinadas em operações, função da característica da nossa intervenção ao nível das operações de CSI, de GE e de Ciberdefesa.

7. Tendo estado ligado à formação quer no Instituto de Estudos Superiores Militares como na Escola das Armas, que componentes vê com maior importância para a formação de um futuro Oficial de Transmissões?

Para o futuro oficial de Transmissões, seja numa fase mais inicial da sua carreira, onde a Escola das Armas e o seu polo de formação Regimento de Transmissões assumem particular relevância, ou mais tarde, aprofundando estudos no Instituto Universitário Militar ou na AM, teremos que evoluir nos saberes ao nível da condução de operações militares terrestres e das tecnologias emergentes e disruptivas que potencialmente introduziremos nos sistemas equipamentos da Força Terrestre de Nova Geração do Exército num futuro não muito distante, integrando rapidamente nesse conhecimento as lições que nos chegam dos novos teatros de guerra deste século. Paralelamente, continuar a investir no reforçar das qualificações ao nível do emprego da guerra eletrónica e da ciberdefesa, bem como das operações de comunicações e sistemas de informação em operações conjuntas e combinadas multidomínio. Num ponto de vista mais abrangente, potencialmente na Academia Militar, investir no conhecimento ao nível dos desafios e riscos inerentes à inevitável incorporação crescente de tecnologias de inteligência artificial nos diversos sistemas e equipamentos militares, de forma generalizada e transversal às diferentes funções de combate.

8. Quais foram os principais desafios técnicos e logísticos que enfrentou como Chefe da IT Cell no Quartel General da Missão de Monitorização da Comunidade Europeia (ECMM) na ex-Jugoslávia, especialmente num ambiente como Sarajevo durante aquele período?

No 1.º semestre de 2000, período em que lá estive, o ambiente de segurança geral nos Balcãs estava já significativamente controlado, apenas se encontrando vedado o acesso ao território da Servia e existindo um controlo fronteiriço bastante robusto, mesmo para os elementos da missão, no acesso ao Kosovo. Para a *IT Cell* o principal desafio tecnológico na altura estava relacionado com o incremento da flexibilidade e agilidade dos observadores, com a necessária adaptação dos gabinetes locais e regionais para a utilização de tecnologias sem fio, bem

como a necessidade de comunicação permanente entre todos as equipas e gabinetes no terreno com o Quartel-General em Sarajevo para a comunicação segura diária (relatório) para Bruxelas. Durante o meu período na missão, correspondente à presidência portuguesa do Conselho Europeu e tendo como senior nacional o então Cor Tm Rui Rodrigues, tivemos a oportunidade de definir os requisitos técnicos para a nova arquitetura CSI dos gabinetes regionais e ainda implementar o novo espaço na Macedónia. Quanto à componente logística da missão, esta funcionava extremamente bem. A IT Cell respondia neste âmbito ao *branch* das comunicações, onde estava também o então Cap Tm Sousa e Silva, e o orçamento que tínhamos disponível permitia almejar obter em tempo as mais inovadoras tecnologias à data, apoiados por um *staff* de jovens engenheiros e técnicos locais muito competente, resultante da vantagem competitiva da capacidade de contratação da missão face às condições do mercado local, o que facilitou em muito a minha tarefa.

9. Dada a crescente importância de salvaguardar o ciberespaço e a evolução constante das ameaças cibernéticas, considera pertinente a implementação de um novo curso complementar ao tradicional de Transmissões, com foco mais direcionado para as áreas de Engenharia Informática e Cibersegurança?

Como referi anteriormente, e como já aconteceu no passado com a Engenharia de Sistemas e *Software*, creio que o curso tinha esta designação, existe abertura e estudos estão a ser feitos para o eventual alargamento das opções na formação inicial para o Quadro Especial de Transmissões, nomeadamente no Instituto Superior Técnico para os oficiais, mas também ao nível dos Cursos Técnicos Superiores Profissionais para os Sargentos, como referi antes, designadamente com a possibilidade de ingresso direto de civis na ESE já com habilitação CTSP Nível 5. Penso ser uma evolução natural resultante da relevância crescente do novo domínio operacional ciberespaço para a condução de operações militares, que, face à convergência e maturidade tecnológica que se espera alcançar em meados da próxima década, designadamente ao nível da hiper conetividade da nossa sociedade, da adoção generalizada de inteligência artificial e da computação quântica, terá tendência para acelerar ainda mais a relevância do nosso contributo para o sucesso das missões atribuídas ao Exército.

Creio que o importante na formação de base de um Oficial de Transmissões é dotá-lo das melhores ferramentas que lhe permitam, à medida que se for deparando com novos desafios, procurar e agregar diferentes áreas do conhecimento tecnológico no âmbito das comunicações e dos sistemas de informação, bem como, capacitá-lo para conhecer a fundo as suas características técnicas e o potencial para o seu emprego em operações militares. A velocidade atual da inovação e da evolução tecnológica obriga-nos a um esforço individual permanente no acompanhamento e atualização, pelo que o importante será que a formação inicial seja de enorme qualidade e que nos permita manter uma solida e coerente estrutura base de conhecimento e método para o fazermos. A formação académica inicial proporciona-nos estas ferramentas necessárias para, ao longo da vida, podermos continuar a aprender e a evoluir o nosso conhecimento, e daí o do Exército, seja através de ações de ensino e/ou de formação formais, seja pela autoaprendizagem e pela capacidade de motivação individual para aprender e ensinar os que connosco trabalham. Creio que isso será o mais importante, não esquecendo que, enquanto oficiais do Quadro Permanente, é nossa obrigação continuar a aprender para conseguir motivar e desafiar a fazer sempre melhor aqueles que connosco vão cumprir as missões que nos confiarem, rumo ao Exército credível, moderno, atrativo, de elevada prontidão e competência que todos ambicionamos manter e ajudar a evoluir.

10. Quais são as principais diferenças entre uma FND e um cargo NATO no que diz respeito à organização, às atividades do dia a dia e às responsabilidades específicas de um Oficial de Transmissões?

Numa Força Nacional Destacada (FND) estamos inseridos na estrutura militar típica de uma unidade de determinado escalão, cumprindo a nossa ação, na maioria dos casos, ao apoio e à execução de funções e tarefas de acordo com a missão de natureza tática e características do Teatro de Operações onde a mesma está inserida. Recentemente, nas Transmissões, temos assegurado Destacamentos CSI nas diversas FND, onde o Oficial de Transmissões assume a sua chefia e assegura que todo o apoio CSI à Força é prestado, desde o planeamento à execução, apoiando o seu Comandante e os elementos de Estado-Maior em tudo o que sejam assuntos específicos e responsabilidade de Tm, bem como na manutenção da ligação às diferentes unidades de Tm em Território Nacional com intervenção no apoio de retaguarda à Força. Atualmente não temos tido participação como unidades constituídas de Tm, como foi o caso da primeira FND do Exército após a guerra do ultramar, em 1993, com a constituição e projeção do BTm5 para Moçambique, ou mais tarde da CTm4 para Angola, mas creio que será legítimo ambicionar vir a ter novamente no futuro uma realidade idêntica, designadamente em resultado da capacitação em curso e da concretização os projetos TDCIS, GE e CD *Deploy*.

Num cargo, na NATO, na EU ou na ONU, na sua maioria dos casos correspondente ao desempenho de funções de estado-maior num grande comando ou organismo. Na sua maioria dos casos, a indigitação para estes cargos prevê a existência de habilitação com o Curso de Estado-Maior, curso a que nos podemos candidatar após o Curso de Promoção a Oficial Superior, existindo também cargos de natureza mais técnica, de determinada Área Funcional, onde poderão ser apenas outras competências específicas que ditarão o processo de seleção, indigitação e posterior nomeação, dependendo as funções e tarefas a desempenhar da divisão/área onde se prestará serviço.

No meu caso específico: na ECMM/EUMM, na Bósnia, estive numa estrutura de missão equivalente a um comando operacional, onde as minhas funções eram de chefia de uma secção de informática, numa Divisão chefiada por Cor Tm do Exército alemão, apoiando o Quartel-General da missão e os diferentes gabinetes e sites da equipas de observadores distribuídas pelos Balcãs; No *HQ Southlant/ JFC Lisbon*, em Oeiras, na Divisão de Comunicações (J6) chefiada por Cor Tm do Exército americano, desempenhei funções típicas de chefia de uma secção de informática, focada no *Helpdesk* a um grande comando NATO; Na NC3A, atual NCIA, estava inserido numa *Capability Area Team* para a área da Engenharia de Sistemas, chefiada por um civil (eramos cerca de 60 militares em aproximadamente 600 elementos da agência), antigo Maj Tm do Exército americano, assegurando essencialmente a gestão de projetos, como foi o caso da industrialização do *Tasker Tracker Enterprise* e respetiva instalação em todos os comandos NATO, cujo contrato para o desenvolvimento de software com a Microsoft Bélgica foi elaborado e negociado pelo meu antecessor, então TCor Tm Guilherme, e aguardava apenas a assinatura final pela Agência no momento em que me apresentei, assumindo então o projeto na sua fase de execução, com a transferência de conhecimento da NC3A para a Microsoft para o desenvolvimento do *software*, acompanhando posteriormente todos os testes de verificação e validação para poder ser utilizado na rede classificada da NATO, e a instalação e formação nos diferentes comandos.

11. Com o avanço de tecnologias como inteligência artificial e comunicações 5G, como acredita que essas inovações podem ser integradas na Arma de Transmissões, e quais os desafios para a sua adoção?

Não só acredito, sou oriundo de uma Arma onde a inovação e a adoção de novas tecnologias

sempre esteve no ADN de quem nela serviu e serve, como vos posso assegurar que nestes dois casos em concreto está a acontecer neste momento. Temos soluções com recurso a tecnologias de Inteligência Artificial (IA), como referi antes, na implementação do primeiro piloto de utilização on premises LLM, tendo também o Comando do Pessoal efetuado no ano passado uma prova de conceito com a Microsoft nesta área da utilização de ferramentas de IA, neste caso com recurso à *Cloud* da empresa, e na adoção das tecnologias 5G com duas áreas, a aquisição em curso de sistemas e equipamentos para emprego no apoio a operações civis, uma comummente designada "bolha tática", bem como com o projeto para a sua adoção no incremento da segurança das nossas unidades. O nosso desafio, entre aspas, reside na necessidade de inverter a nossa aparente menor apetência para "vender" o produto do nosso trabalho, valorizar os nossos sucessos, por mais pequenos que sejam!

Os desafios hoje prendem-se essencialmente com a capacidade que temos em cada momento, leia-se pessoas que integram a nossa equipa, para conseguirmos fazer o trabalho que temos de desenvolver aos diferentes níveis de gestão, ou seja, para a execução, protegendo e mantendo toda a estrutura a funcionar 24/7, para o acompanhamento da evolução da inovação e da indústria, bem como para o planeamento de médio e longo prazo do Exército para as áreas tecnológicas da responsabilidade das Transmissões.

12. Como vê a importância da interoperabilidade entre as Transmissões e outras Armas e Ramos das Forças Armadas, e quais são as áreas mais críticas para fortalecer essa integração?

Alcançar a plena interoperabilidade no âmbito das comunicações e dos sistemas de informação modernos, não apenas a nível conjunto nacional, mas também nas diferentes organizações internacionais de que Portugal faz parte, sendo a NATO uma das principais impulsionadoras deste imperativo das operações envolvendo Forças de diferentes Nações Aliadas é fundamental. Portugal, e o Exército em particular, tem promovido este incremento da interoperabilidade, designadamente ratificando acordos de estandardização da NATO (STANAG) e exigindo o seu cumprimento pelos fornecedores através da sua inclusão nos requisitos técnicos em novas aquisições. Mas não ficamos apenas por aqui, juntamente com o EMGFA, que está a desenvolver um excelente trabalho na coordenação nacional para acompanhar a evolução e a certificação da conformidade das nossas redes, sistemas e serviços a nível operacional e tático com os requisitos definidos pela *framework Federated Mission Network* (FMN), investimos anualmente na participação no maior exercício de interoperabilidade da NATO, o *Coalition Warrior Interoperability Exercise* (CWIX), onde, inclusivamente com representantes de empresas nossas fornecedoras, ou parceiras em projetos de investigação, testamos e validamos os nossos atuais e futuros sistemas e equipamentos diretamente com os de outras Nações. Os nossos camaradas da equipa de Engenharia para o Projeto SIC-T da DCI assumem aqui uma extraordinária relevância, sendo normalmente reforçados durante a fase LIVEX do exercício com elementos do RTm, não apenas a nível da preparação da participação nacional, mas também assumindo alguns dos seus oficiais papeis de liderança em áreas específicas das estruturas de teste e validação do CWIX, face ao reconhecimento internacional inter pares das suas competências e da grande experiência que detêm, pois esta equipa faz hoje a ligação e o acompanhamento próximo às equipas de projeto de diferentes capacidades para todas as tecnologias que necessitem de comunicações ou sistemas de informação a nível tático.

Neste âmbito, tem sido igualmente promovida a participação de elementos de outros órgãos do Exército em áreas de teste de interoperabilidade do CWIX, para além das puramente CIS da responsabilidade das Transmissões, onde saliento a participação do CIGeoE com o SIGOp na área Geoespacial e do CFT no LAND.

Saliento que o empenhamento do Exército em alcançar a interoperabilidade internacional dos seus sistemas não é de hoje, recordo que nos finais do século passado, com o Sistema de Informação de C2 do Exército (SICCE), o Exército liderava neste âmbito da interoperabilidade entre ferramentas de C2 ao nível dos requisitos definidos pelo *Multilateral Interoperability Programme* (MIP), creio que até à versão 3.0 ou 3.1, integrando um grupo de trabalho com exércitos das nações da NATO e europeias para assegurar a interoperabilidade do que hoje se designa de *Headquarters Management Systems* (HMS) para escalão Batalhão e superior.

Apesar de todo este trabalho, ainda temos um longo caminho a percorrer, principalmente pelo facto de ser necessário alcançar hoje elevados níveis de interoperabilidade aos escalões mais baixos, como Pelotão, ao contrário do passado recente, em que esta preocupação se focava no nível Agrupamento/ Batalhão e superior, sendo assumido que níveis inferiores seriam essencialmente assegurados pelos respetivos sistemas da Nação que fornecia a Força. Atualmente é comum projetar uma FND de escalão SubAgrupamento ou Companhia, ou mesmo até Pelotão, levando assim este desafio para o patamar das Redes Rádio de Combate, e em particular para a sua vertente da transmissão segura, onde se pretende evoluir para equipamentos com arquiteturas *Software Defined Radio* (SDR) que permitam, conforme a Força ou missão que integremos, o carregamento de formas de onda comuns nos equipamentos rádio de múltiplos fornecedores que equipam as diferentes Forças, eventualmente desenhadas especificamente para a respetiva missão que integram.

13. Que legado gostaria de deixar na Arma de Transmissões e qual a sua visão sobre como ela deve evoluir para enfrentar os desafios das próximas décadas?

Naturalmente que temos de evoluir, principalmente porque, como referi no início, estamos debaixo de enorme pressão, olhando ao que considero ser o principal condicionante da nossa atividade atual, a exiguidade de Recursos Humanos. Este fator limita a capacidade de concretização do potencial diferenciador que o nosso Quadro Especial oferece ao Comandante do Exército no esforço coletivo de ajudá-lo a alcançar a sua visão.

Mas nessa exiguidade, ressalta uma certeza, as novas gerações que entram no Quadro Especial de Transmissões, apesar de em número muito inferior às reais necessidades do Exército, estão hoje tecnicamente muito bem preparadas para os desafios que vão encontrar no início da sua carreira. Esta afirmação é confirmada pela observação interna, mas também pelas constantes manifestações de reconhecimento por entidades externas, militares e civis, seja nas missões, em exercícios ou em projetos e grupos de trabalho nacionais e internacionais.

Para vencer os desafios do presente e melhor construir o futuro, há naturalmente trabalho interno a evoluir. Importa conseguir melhorar no período inicial de carreira as condições para a obtenção da necessária experiência militar pelos camaradas mais modernos, em particular os oficiais, para os quais o equilíbrio entre o saber ser militar e simultaneamente ser engenheiro é crucial. Este trabalho deve ser alicerçado no exemplo e numa ação de comando próxima e efetiva, que lhes permitam obter igual nível de competências profissionais e alcançar com celeridade elevada proficiência no âmbito da execução das suas tarefas. É uma fase extraordinária, de nos envolvermos na prática em diferentes áreas de atuação da Arma, assumindo responsabilidades de comando e de liderança sobre outros camaradas que connosco irão cumprir determinada missão e respetivas tarefas, identificando ou confirmando aquelas áreas com que melhor nos identificamos, e eventualmente em torno das quais procuraremos moldar o futuro da nossa carreira.

De igual forma, é imperioso continuar a incentivar os comandantes e chefes para proporcionar condições e espaços nas absorventes atividades do dia a dia para permitir olhar para além do horizonte, obrigando-nos "a levantar a cabeça do teclado", incentivando a participação em eventos e sessões para debater novas ideias, estudar e procurar tecnologias inovadoras, para propor de forma sustentada

e estruturada projetos e soluções que permitam ultrapassar alguns dos muitos desafios identificados pelas diferentes Unidades e estruturas do Exército, bem como procurar trabalhar mais de perto com as novas estruturas do Exército na área da Experimentação, da Inovação e da Capacitação Tática e Simulação, incrementando o seu potencial para o estabelecimento de pontes com a Industria e a Academia para o estabelecimento de novos projetos com o Exército, designadamente envolvendo áreas da nossa responsabilidade.

14. Que mensagem gostaria de deixar para todos os militares das Transmissões e, em particular, aos recém-chegados à Arma de Transmissões?

Reforço a mensagem de confiança na qualidade da formação que o Exército ministra, dotando os recém-chegados das melhores ferramentas e valores para iniciarem a fase mais interessante da carreira, o desempenho das funções de subalterno. É um momento de descoberta e de afirmação, onde irão desenvolver a arte de comandar pelo exemplo e consolidar as competências de liderança dos homens e das mulheres colocados sob a vossa responsabilidade, integrando-se na cultura própria da instituição militar, que se adquire na vivência diária e na comunhão de princípios e valores comuns, pelo que vos exorto também a estarem individualmente predispostos a abraçá-la e a cultivá-la. Salientaria ainda o facto de, independentemente das competências técnicas, graus académicos e postos, mantenham sempre a consciência de "saber que nada sabem", continuando a cultivar a capacidade para aprender ao longo da vida, expandindo o vosso conhecimento e o do Exército. Com essa forma de estar, e vontade, no mesmo Exército que, com a vossa participação ativa se constitui como "um mundo de oportunidades" para as empresas nacionais, estou certo de que todos terão competências e igualmente as oportunidades e o terreno ideal para, onde quer que prestem serviço, poderem aplicar esse conhecimento em projetos e iniciativas que tragam inovação e integração de novas tecnologias para ajudar as vossas unidades a melhor cumprir a sua missão.

Para todos, em especial para os mais antigos, muito em resultado da minha recente passagem pelas funções de Diretor da DCI e de Presidente do Conselho da Arma, deixo a certeza e a confiança que tenho na capacidade de trabalho dos poucos, mas, eventualmente também em resultado disso, muito bons homens e mulheres que servem hoje no Exército na Arma de Transmissões. Dito assim, parece um lugar-comum… mas não o pretende ser, é sentido! Acreditem mais nas vossas capacidades individuais para abraçar áreas novas, e desenvolvam a arte de melhor comunicar o excelente trabalho coletivo que é feito aos diferentes escalões e áreas da atuação da Arma.

A honra e o privilégio que consiste em comandar uma unidade ou órgão do Exército é algo particularmente intenso, assumindo sempre inúmeros desafios, diferentes em cada momento do tempo, mas sempre com uma constante… quando, entre camaradas e amigos, revisitamos as nossos histórias, os tempos mais desafiantes e exigentes aconteceram sempre naquele que foi "o nosso tempo"! Confirmo, concluindo e expressando um profundo agradecimento a todos pelo trabalho que realizam diariamente, muito em particular à muito eficaz equipa que comigo serviu na DCI, exortando-vos a continuar a alimentar a vossa paixão pelas respetivas áreas de competência, a manter a elevada dedicação e a grande generosidade pessoal que caracteriza os militares da Arma de Transmissões, continuando a desenvolver excelente trabalho em cada uma das nossas múltiplas áreas de intervenção, nas comunicações e nos sistemas de informação, na guerra eletrónica, na ciberdefesa, na gestão da informação e do conhecimento, seja a nível tático como fixo, ultrapassando sempre os inúmeros desafios diários quotidianos, acompanhando as tendências e preparando o futuro para, com grande abnegação, melhor apoiarem os vossos Comandantes no cumprimento das respetivas missões.

Bem hajam, Forte Abraço a todos.

Redes Seguras – Distribuição Quântica de Chaves

Tenente-Coronel Tm Pedro Fernandes
Comandante do Grupo de Operações no Ciberespaço
Centro de Guerra de Informação e Ciberespaço (CGIC)

Introdução

A segurança dos nossos Sistemas de Informação e Comunicações (SIC) baseia-se essencialmente na complexidade computacional, pelo que são vulneráveis aos avanços da capacidade computacional e dos algoritmos. Deste modo, os nossos sistemas atuais podem ser vulneráveis a qualquer pessoa que tenha acesso a um computador quântico.

Em 7 de junho de 2024, as Nações Unidas proclamaram 2025 como o Ano Internacional da Ciência e Tecnologias Quânticas (*IYQ - Year of Quantum Science and Technology*) por forma a reconhecer os 100 anos do desenvolvimento inicial da mecânica quântica [1]. Portanto, este tema parece bastante pertinente e atual pelo que vamo-nos debruçar sobre ele, aqui na perspetiva da criptografia quântica.

Com efeito, com a ameaça iminente dos computadores quânticos, a necessidade de métodos de encriptação robustos nunca foi tão crítica. A sua segurança passa pela utilização também de tecnologias quânticas aplicadas à área cripto. Assim, existem fundamentalmente duas abordagens diferentes: a abordagem clássica e a abordagem quântica. A abordagem clássica tenta desenvolver uma criptografia pública mais robusta e abordagem quântica evita, de todo, a utilização de criptografia pública. Portanto, temos o conceito de criptografia pós quântica, em inglês *Post-Quantum Cryptography* (PQC), e o conceito de distribuição quântica de chaves, em inglês *Quantum Key Distribution (QKD)*, também chamado simplesmente de criptografia quântica.

Ambas as abordagens têm prós e contras, mas, haverá cenários em que a criptografia clássica pós-quântica (PQC) será suficientemente robusta e rápida, e outros em que a criptografia quântica (QKD) terá a praticidade adequada para ser usada. Haverá ainda outros cenários em que uma mistura de ambas as abordagens oferecerá a melhor solução.

Neste artigo vamos analisar apenas a QKD, concretizando com o caso português.

Conceito

Os métodos de encriptação atuais baseiam-se na utilização de chaves simétricas e assimétricas. A criptografia quântica (QKD) aplica-se às chaves simétricas. Neste tipo de criptografia, também conhecida como criptografia de chave secreta, a mesma chave é utilizada tanto para cifrar como para decifrar os dados. Um dos principais desafios é como distribuir com segurança a chave secreta para as partes que precisam dela. Se a chave for intercetada por uma parte não autorizada, esta pode decifrar as mensagens.

Por conseguinte, uma solução pode passar por distribuir as chaves criptográficas utilizando recursos quânticos.

Figura 1 – Transmissão segura de uma mensagem

Vamos então mergulhar uma pouco mais na importância da distribuição quântica de chaves. Por um lado, a sua segurança pode ser independente dos algoritmos ou dos avanços da potência computacional (incluindo os computadores quânticos), e por outro lado, pode evitar a utilização de criptografia pública. Também, devido às propriedades fundamentais dos sistemas quânticos, este método permite a deteção de ataques *Man-in-the-Middle* (MITM) tradicionais com elevada eficiência. Portanto, ao contrário dos métodos de criptografia clássica, que dependem da complexidade computacional, a QKD oferece segurança incondicional, oferecendo uma encriptação teoricamente inquebrável. Desta forma, trata-se de um conceito promissor para implementação de redes seguras em contexto militar..

Projetos em curso

Figura 2 – Projetos em curso

A iniciativa Infraestrutura Europeia de Comunicação Quântica *(EuroQCI - European Quantum Communication Infrastructure)* visa construir uma infraestrutura de comunicação quântica segura, que abrangerá toda a União Europeia, incluindo os seus territórios ultramarinos. Foi lançada em 2019 e baseia-se nas tecnologias inovadoras de comunicação quântica. A componente portuguesa com o nome de PTQCI (*Portuguese Quantum Communications Infrastructure*) [2], com uma implementação já testada em Lisboa, visa criar uma rede quântica avançada de apoio às iniciativas nacionais de comunicação quântica e sua integração com as redes de comunicações existentes.

Já o projeto europeu de nome DISCRETION *(Disruptive SDN Secure Communications for European Defence)* [3], liderado por Portugal, constitui-se como pioneiro para desenvolver redes de comunicação quântica para a Defesa e procura fornecer, pela primeira vez, serviços de encriptação de alta segurança de última geração. Aborda a ameaça da computação quântica utilizando tecnologias disruptivas como *Software Defined Networks (SDN)* e *Quantum Key Distribution (QKD)* para criar uma rede de comunicações segura e resiliente para as forças militares europeias. Fazendo uso das redes óticas já existentes, o *DISCRETION* permitirá construir uma rede altamente segura, escalável e resiliente para serviços operacionais táticos avançados.

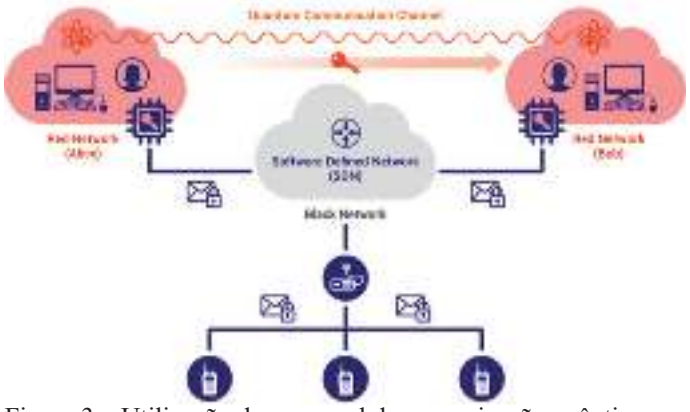


Figura 3 – Utilização de um canal de comunicação quântica

De realçar que dos parceiros do *DISCRETION* consta o Estado-Maior General das Forças Armadas (EMGFA) e o Gabinete Nacional de Segurança (GNS) que investiram neste projeto. O Exército tem participado, pontualmente, em alguns eventos tendo vindo a dar contributos quando solicitado. Dependendo dos resultados alcançados e da viabilidade demostrada deverá o Exército integrar os futuros desenvolvimentos nesta matéria.

Principais desafios

Apesar da QKD se apresentar como uma tecnologia promissora, muitos são os desafios que será necessário vencer para tirar partido da mesma. Destes, destacam-se as seguintes questões que necessitam de resposta futura:

1) Escalabilidade: Como expandir as redes QKD para atender as necessidades operacionais?

2) Resistência a Ataques: Será a QKD suficientemente segura? Como detetar e prevenir ataques?

3) Integração com Infraestrutura Existente: Como incorporar QKD em sistemas militares já existentes?

Figura 4 – Implementação em laboratório de comunicações quânticas
Instituto de Telecomunicações / Universidade de Aveiro

Há ainda que ter em consideração que, devido custo do hardware, a implementação desta tecnologia pode ser extremamente cara, quer para o seu estudo ao nível académico, quer ao nível comercial. A considerar ainda outras limitações, como seja o facto da QKD só funcionar com comunicações óticas (fibra ou espaço livre).

Em suma, apesar de promissora são muitos ainda os desafios que necessitam ser ultrapassados para efetivamente colocar a tecnologia QKD ao serviço das Forças Armadas.

Conclusões

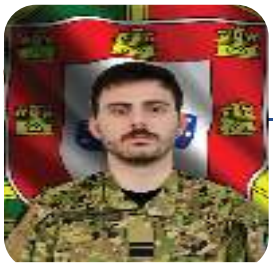
Quando os computadores quânticos forem capazes de violar a criptografia moderna, serão necessárias novas formas para manter a comunicação segura. Assim, a Distribuição Quântica de Chaves (QKD) é uma das abordagens que utiliza os princípios da mecânica quântica para estabelecer canais de comunicação seguros e que oferece segurança incondicional com base nas propriedades fundamentais dos sistemas quânticos com uma encriptação teoricamente inquebrável.

Existem presentemente em curso diversos projetos a nível europeu do qual se destaca o projeto *DISCRETION*, liderado por Portugal, que conta com a participação do EMGFA e GNS. Este visa desenvolver redes de comunicação quântica para a Defesa e procura fornecer, pela primeira vez, serviços de encriptação de alta segurança de última geração utilizando QKD. Contudo, embora tenham muito potencial, é necessário acompanhar os desenvolvimentos futuros e perceber se a segurança oferecida versus custos e limitações são adequados para incorporação desta tecnologia no Exército.

Mas uma coisa é certa, é preciso estar atento e tomar as decisões certas no tempo adequado para nos mantermos na "crista da onda" e acima de tudo garantir o nível de segurança adequado nas redes seguras militares.

Referências bibliográficas

[1] https://quantum2025.org
[2] https://ptqci.pt
[3] https://discretion-eu.com



Implementação de uma arquitetura *Zero Trust*

Capitão Tm Hélder Reia
Chefe no Núcleo de Monitorização e Análise e do Núcleo de Resposta a Incidentes

Pilares da arquitetura *Zero Trust*

Nos dias de hoje, em que as ameaças no ciberespaço evoluem constantemente, tornando insuficiente as abordagens tradicionais de segurança, baseadas em perímetros, com a abordagem de defesa em profundidade. A arquitetura *Zero Trust* surge como uma resposta estratégica a esse desafio, redefinindo os conceitos de confiança na segurança da informação.

Esta arquitetura baseia-se no princípio de que nenhuma entidade deve ser automaticamente confiável e que qualquer parte da rede pode ser comprometida a qualquer momento. Assim, a segurança não está associada a um perímetro físico ou lógico, mas é aplicada diretamente onde estão os ativos mais valiosos: os dados e os recursos.

Deste modo, a arquitetura *Zero Trust* representa a mudança do paradigma de segurança, colocando o foco na proteção de utilizadores, recursos e dados, independentemente de onde estejam inseridos.

Pilares da arquitetura *Zero Trust*

A arquitetura *Zero Trust*, definida pela *Cybersecurity and Infrastructure Security Agency* (CISA[1]), estrutura-se em torno de cinco pilares fundamentais que orientam a sua implementação. Cada um destes pilares desempenha um papel essencial na construção de um ambiente seguro e resiliente, onde a confiança não é presumida, mas verificada continuamente. Estes pilares são: Identidade, Dispositivos, Redes, Aplicações e *Workloads* e Dados.

Uma identidade consiste numa coleção de informações que distingue de forma inequívoca um utilizador ou entidade dentro de um sistema. Esses atributos podem incluir, mas não se limitam a:

• Utilizadores humanos: Nome de utilizador, endereço de e-mail, número de identificação ou outros dados pessoais.

• Entidades não humanas: Identificadores de dispositivos, certificados digitais, chaves API ou nomes de aplicações.

A identidade é o ponto de partida para todas as decisões de acesso dentro de uma arquitetura *Zero Trust*. Cada vez que um utilizador ou entidade tenta interagir com um recurso, a identidade deve ser rigorosamente validada através de:

• Autenticação Multi-Fator (MFA): Garantindo que a identidade é legítima;

• Gestão de Identidade e Acesso *(Identity and Access Management - IAM)*: Concedendo apenas o acesso à informação estritamente necessária;

• Monitorização Contínua: Verificando o comportamento da identidade em tempo real para identificar desvios ou atividades suspeitas.

[1] - https://www.cisa.gov/zero-trust-maturity-model

Figura 1 - Tipos de Autenticações Multi-Fator

Um dispositivo é qualquer ativo para a organização, sendo *hardware* ou *software*, que seja utilizado para a ligação à rede, incluindo servidores, computadores fixos e portáteis, dispositivos móveis, impressoras, equipamentos de rede, entre outros. Por forma a garantir a segurança constituinte deste pilar, deve ser garantido:

• **Inventário de dispositivos:** Manutenção de uma lista atualizada de todos os dispositivos que interagem com os sistemas;

• **Gestão de dispositivos móveis (MDM):** Implementação de políticas de segurança para dispositivos móveis e endpoints;

• **Monitorização de integridade:** Avaliação contínua do estado de segurança dos dispositivos, garantindo que estão atualizados e não comprometidos.

Embora o modelo Zero Trust elimine o conceito de confiança implícita dentro das redes, este pilar foca-se na segmentação e proteção do tráfego de rede. As principais práticas incluem:

• **Segmentação de rede:** Divisão da rede em segmentos menores para limitar o movimento lateral em caso de compromisso;

• **Criptografia de tráfego:** Uso de protocolos como TLS para proteger comunicações internas e externas;

• **Monitorização de tráfego:** Implementação de sistemas que detetam atividades anómalas ou potencialmente maliciosas.

As aplicações e os *workloads* são frequentemente alvos críticos e, como tal, propícios a ciberataques. Este pilar concentra-se na segurança das aplicações, desde o desenvolvimento até à operação. Os aspetos críticos incluem:

• **Gestão de acessos a aplicações:** Garantir que apenas utilizadores autenticados podem interagir com aplicações sensíveis;

• **Análise de vulnerabilidades:** Identificação e mitigação proativa de falhas de segurança nas aplicações;

• **Ambientes isolados:** Implementação de medidas de contenção que impedem a propagação de ataques dentro das aplicações;

• **Orquestração de Políticas:** Coordenação de políticas de segurança através de diferentes domínios e sistemas.

Os dados são o núcleo de qualquer organização e o pilar central a arquitetura *Zero Trust* garante que são protegidos de forma robusta, independentemente de onde estejam armazenados ou processados. As práticas incluem:

• **Classificação de dados:** Identificação e categorização dos dados com base na sua sensibilidade;

• **Controlo de acessos baseado em contexto:** Garantir que apenas utilizadores e dispositivos autorizados podem interagir com dados específicos;

• **Encriptação e tokenização:** Proteção dos dados em repouso, em trânsito e em uso para reduzir o risco de exposição.

Figura 2 - Segregação de Acesso aos Dados

Como deve o Exército abordar uma arquitetura *Zero Trust*?

Com o crescente de tecnologia presente nas redes e sistemas do Exército, bem como no acesso mais global e através de acessos remotos, cada vez mais se estuda as opções da migração de alguns serviços para a *Cloud*. Para além disto, muitas aplicações e serviços focam esta mesma migração, dado a estratégias organizacionais e custos associados.

A implementação de uma arquitetura *Zero Trust* é essencial para qualquer organização que procure fortalecer a sua postura de segurança, especialmente antes de integrar soluções baseadas na *Cloud* ou conectá-las a redes externas. Adotar este modelo antes de avançar para esses passos é uma decisão estratégica que protege a organização de vulnerabilidades inerentes às infraestruturas tradicionais e às ameaças emergentes e que tem de ser feito antes da migração de serviços e dados para a *Cloud*.

Figura 3 - Transição de Serviços *On-premise* para *Cloud*

Numa implementação de uma arquitetura *Zero Trust*, ninguém está acima das regras de segurança. Permitir exceções para utilizadores específicos enfraquece a integridade do sistema e cria lacunas que podem ser exploradas por atores maliciosos. Como tal, deve ser considerado que todos utilizadores são potenciais vetores de ataque pois podem, sem querer, comprometer a segurança devido a credenciais roubadas ou através de campanhas de *phishing*.

Posto este pressuposto, devem-se evitar privilégios excessivos pois estas exceções podem levar a níveis de acesso desnecessariamente altos, aumentando o risco de movimentos laterais dentro da rede em caso de comprometimento. A arquitetura *Zero Trust* exige, também, que todos os acessos sejam validados, independentemente do cargo, função ou localização.

Como é possível ver na Figura 4, deve também existir planeamento do ponto de vista de utilização dos serviços e da segurança numa fase de transição. Os serviços e dados devem ser migrados de forma estudada, existindo uma fase de transição, onde o acesso aos mesmos deve ser feito de forma limitada e os controlos de segurança devem já estar configurados. Como objetivo, o Exército Português deve estabelecer as políticas que garantam a segurança descrita nos pilares da arquitetura *Zero Trust*.

Figura 4 - Arquitetura de Transição

Conclusões

No contexto da cibersegurança moderna, as tecnologias e princípios subjacentes à arquitetura de *Zero Trust*, conforme detalhado na *Zero Trust Reference Architecture do* Department of Defense (DoD), são amplamente reconhecidos e utilizados. Estas tecnologias, que incluem autenticação multifator, gestão de identidades e acessos, micro-segmentação, criptografia, monitorização contínua, entre outras, já são conhecidas e implementadas em várias organizações para reforçar a segurança dos seus sistemas e dados.

A migração para a *Cloud*, seja em modelo público, privado ou híbrido, deve ser abordada com cautela e planeamento quer estratégico, quer dos sistemas. É essencial que a arquitetura de *Zero Trust* esteja plenamente estabelecida antes de se proceder à migração para a *Cloud*. Ao implementar a arquitetura de *Zero Trust* antes da migração para a *Cloud*, o Exército Português não só aumenta a segurança da sua informação como também melhora o acesso à mesma.

Portanto, o Exército Português deve adotar esta abordagem, por forma a estar melhor preparado para enfrentar as ameaças no ciberespaço e proteger os seus dados digitais num mundo cada vez mais conectado e dependente da tecnologia.

Apesar desta arquitetura de segurança ser já conhecida, verifica-se que o Exército Português deve ainda fazer alguns progressos no ponto de vista da sua implementação.

O papel das Redes Táticas Heterogéneas e das *Coalition Waveforms* nas Operações de Multi-Domínio

Capitão Tm Rui Gomes
Chefe da EqProjSIC-T/DCI
Chefe da Secção de Equipamentos Táticos/RCom

A evolução das operações militares e das tecnologias dos sistemas de comunicações impõem novos desafios para todas as Forças Armadas, principalmente quando se trata de garantir a eficácia das comunicações em cenários de alta complexidade, como em operações conjuntas e combinadas entre diferentes países, nomeadamente em contexto NATO. Neste contexto, as Redes Táticas Heterogéneas (HTNs) e as *Coalition Waveforms* (CWFs) da NATO assumem cada vez mais importância, na medida em que a sua correta implementação, aliada a uma clara estratégia de edificação de capacidades de comunicações e sistemas de informação (CSI), sobretudo de âmbito tático, pode permitir que determinadas forças consigam garantir a interoperabilidade com outras forças aliadas.

Este artigo foca-se no conceito das HTNs e CWFs e como estas podem contribuir para a implementação de sistemas de comunicações eficazes nas operações multinacionais, estabelecendo ainda a relação com os projetos do Exército em que se prevê a sua implementação, apresentando alguns casos práticos e cenários de implementação.

O que são as HTNs?

As HTNs são infraestruturas de comunicações criadas para operar em ambientes de combate ou situações de emergência, onde a conectividade é essencial, mas também onde as condições do terreno e a diversidade de tecnologias tornam a implementação de redes convencionais um grande desafio. Tendo em conta os cenários de atuação de forças militares e do caso particular do Exército Português, esta situação continua a ser vivenciada aos dias de hoje, na medida em que os rádios e as *waveforms* disponíveis nem sempre são compatíveis com os meios que as outras forças aliadas utilizam. De momento a única exceção, em que é possível garantir a interoperabilidade via rádio tático, é quando as comunicações rádio sejam apenas estabelecidas em modo não seguro, considerando apenas modulação FM e apenas serviço de voz, algo que já não é compatível com os cenários atuais do campo de batalha, uma vez que o fluxo de dados é um requisito operacional essencial.

Deste modo, enquanto que as redes táticas tradicionais dependem de uma única tecnologia ou plataforma, as HTNs integram uma variedade de sistemas e tecnologias de comunicações, tais como satélites, rádios de curto e longo alcance, redes móveis, comunicações via internet e até mesmo sistemas de comunicações filares, por exemplo por fibra ótica, DSL, ou outras. Algumas das características principais destas redes são a sua flexibilidade, resiliência e redundância, permitindo que, caso um sistema falhe, outro possa assumir a função sem interromper as comunicações.

Extrapolando este conceito para um caso da sua implementação prática, seguidamente é apresentado um esquema com as ligações previstas entre dois módulos SIC-T no âmbito do projeto TDCIS[1], utilizando sempre a PCN[2] como meio de transporte para interligação dos diversos sistemas de comunicações e diversas tecnologias, tais como sistemas de comunicações interligados por tecnologia filar (WD-1/TT, Fibra Ótica, SFTP), meios rádio *Satcom (Military SATCOM[3] e Commercial SATCOM[4])*, sistemas de comunicações móveis (e.g. GSM, 4G/LTE, 5G), feixes hertzianos (HCLOS[5] e mini-LOS[6]) e por fim rádios táticos *(Narrowband, Broadband)*.

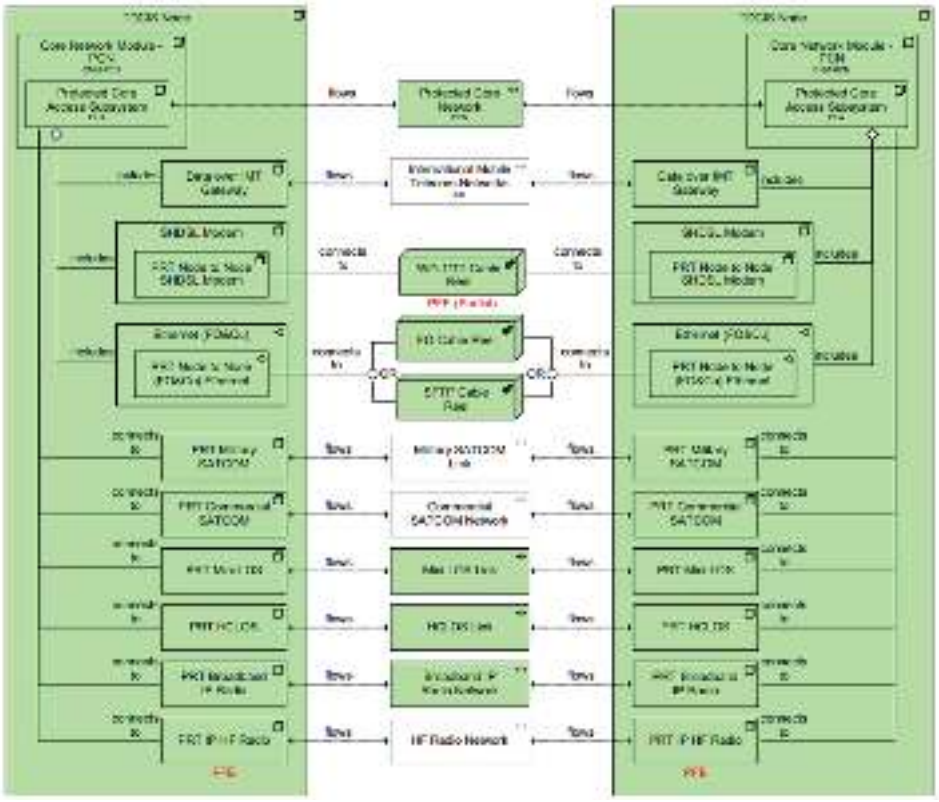


Figura 1 - Possibilidades de interligação entre dois módulos SIC-T, de acordo com a implementação da PCN e dos normativos FMN

A Importância da Interoperabilidade nas Operações da NATO

No contexto da NATO, as HTNs desempenham um papel vital na interligação de diferentes forças aliadas, cujos sistemas de comunicações podem variar consideravelmente em termos de tecnologias e protocolos. A interoperabilidade continua a ser um dos maiores desafios para a NATO e seus aliados, existindo para o efeito o conceito *Federated Mission Networking (FMN)*, para definir todos os processos e mecanismos técnicos que os afiliados devem efetuar para garantir a sua interoperabilidade em todos os serviços previstos pela comunidade FMN, quer sejam de carácter *Core* ou *CoI*[7], nas diversas componentes operacionais *(Maritime, Air, Land, Space, Cyber)*.

---

[1] **TDCIS** – *Tactical Deployable Communications and Information System* – Projeto evolutivo do Sistema de Informação e Comunicações – Tático (SIC-T), com a participação do Exército Português, a *NATO Communications and Information Agency* e a empresa vencedora do concurso internacional – EID S.A.

[2] **PCN** – *Protected Core Networking*

[3] ***Military*** **SATCOM** – Considere-se no âmbito do projeto TDCIS sistemas Satcom que operem nas bandas de frequência X e Ka;

[4] ***Commercial*** **SATCOM** – Considere-se no âmbito do projeto TDCIS sistemas comerciais Satcom equivalentes ao *BGAN Explorer* (*On-the-move*), da rede Inmarsat.

[5] **HCLOS** – *High Capacity Line of Sight*

[6] **Mini-LOS** – Equivalente a sistemas comerciais de feixes do tipo *Wireless Broadband* (e.g. 5 GHz)

[7] **CoI – *Community of Interest*** – Conjunto de diversos serviços de carácter operacional para o apoio das operações (e.g. NIRIS, JOCWatch, NCOP, JChat, etc).

No que toca aos normativos FMN relacionados com as HTNs, apenas surgem instruções técnicas de um serviço específico a partir da Spiral 5, sendo este serviço designado por *Communications Transport* e no qual estão previstas várias tecnologias, várias *waveforms* e outros mecanismos que permitirão aos aliados garantirem a sua interoperabilidade em contexto de implementação de redes de comunicações táticas. Neste momento, no âmbito da participação no FMN CIAV8 Working Group, o Cap Tm Rui Gomes do Exército Português foi nomeado como Service Lead e é o responsável pela criação de todo o catálogo de testes para a validação e verificação da implementação técnica do serviço de Communications Transport, bem como por garantir a gestão do repositório de Test Cases e a sua permanente atualização com base nos contributos de todos os países afiliados FMN.

Neste momento, este é o serviço técnico que é liderado por Portugal, ao nível do grupo de trabalho do CIAV.

Figura 2 - Cenários de emprego do serviço de Communications Transport, aplicado em contexto TACCIS[9] , OPCIS[10] e PCN. Fonte: FMN CPWG[11] - Tactical Edge Syndicate

A interoperabilidade é um requisito fundamental para qualquer missão da NATO, pois as forças aliadas necessitam de partilhar informações cruciais de forma rápida e precisa.

No campo de batalha moderno, o papel das dos sistemas CIS é cada vez mais relevante, na medida em que as falhas nestes sistemas podem por vezes comprometer a eficácia da missão e colocar vidas em risco. A interoperabilidade envolve a capacidade dos diversos sistemas de comunicações, muitas vezes desenvolvidos por fabricantes distintos e em países diferentes, conseguirem comunicar entre si, idealmente sem necessidade de utilização de sistemas intermediários para garantir essa interoperabilidade.

Existem diversas arquiteturas que podem ser consideradas para a implementação da função de roteamento necessária nas HTNs, garantindo a interligação entre todos os nós participantes na rede, nomeadamente *Flat Routing Architecture*, com a possibilidade de co-existirem vários domínios em que são utilizados diferentes protocolos de routing e ainda a arquitetura de *Overlay*, que permite interligar todos estes domínios distintos de forma lógica. Alguns exemplos destas arquiteturas estão apresentados nas figuras a baixo.

Inicialmente é representado um cenário de *Flat Routing Architecture*, no qual existe apenas um *Single Routing Protocol Domain*, com várias tecnologias de trans-

[8] **CIAV** – *Coalition Interoperability Assurance and Validation*
[9] **TACCIS** – *Tactical CIS*
[10] **OPCIS** – *Operational CIS*
[11] **CPWG** – *Capability Planning Working Group*

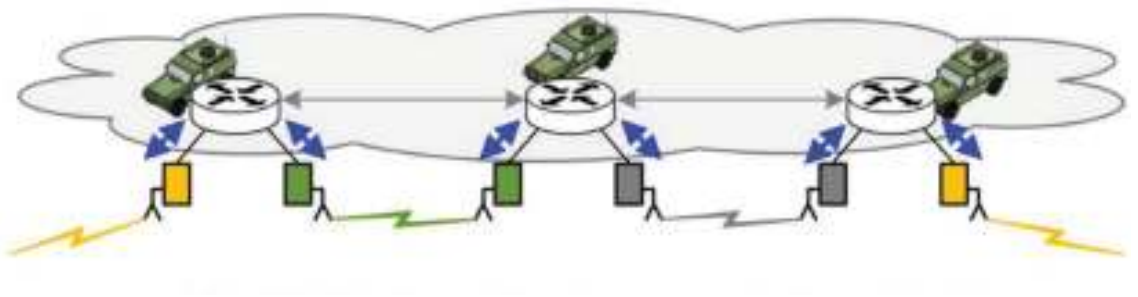


Figura 3 - IEI-M: *Information Exchange Interface - Modem*

Fonte: https://apps.dtic.mil/sti/pdfs/AD1091750.pdf

No cenário seguinte considera-se o mesmo tipo de arquitetura, no entanto neste caso co-existem vários *Routing Protocol Domains*, que se podem interligar entre si através da implementação de *Information Exchange Interface – Routing (IEI-R)*.

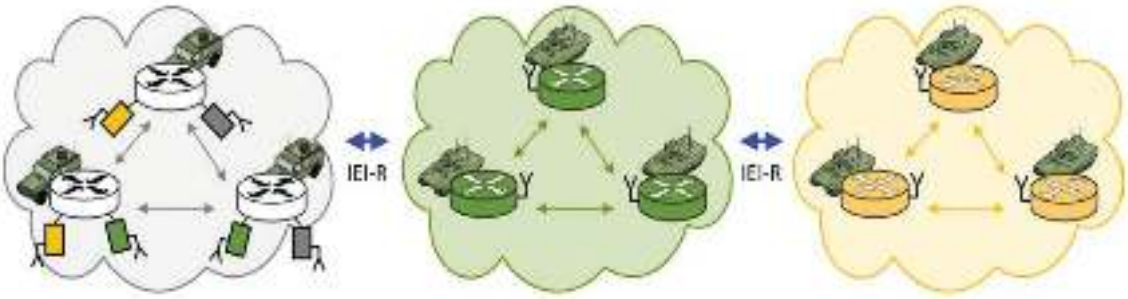


Figura 4 - IEI-R: *Information Exchange interface - Routing*

Fonte: https://apps.dtic.mil/sti/pdfs/AD1091750.pdf

Por fim, no último cenário é apresentada a arquitetura de *Routing Overlay*. Nesta arquitetura, é introduzida uma camada extra de roteamento, que abrange toda a rede heterogénea e interliga todos os diferentes domínios de protocolos de roteamento. Apenas um subconjunto dos routers na rede heterogénea participa nesta camada adicional de roteamento. Estes routers estão localizados nas plataformas de interligação (e.g. viaturas). Este esquema é semelhante à arquitetura que o protocolo *Border Gateway Protocol* (BGP) utiliza para interligar diferentes domínios. Uma *Information Exchange Interface – Routing Overlay* (IEI-RO) é necessária entre o protocolo de roteamento da camada de roteamento adicional e os *Routing Protocol Domains* nos diferentes segmentos de rede. Estes IEI-RO também se encontram nos *routers* das plataformas de interligação. Neste esquema, não existem IEI-Rs entre os diferentes domínios de protocolos de roteamento.

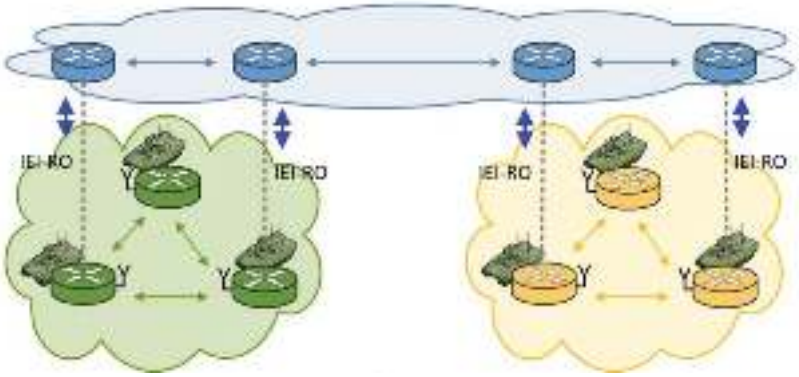


Figura 5 - *Information Exchange Interface - Routing Overlay*

Fonte: https://apps.dtic.mil/sti/pdfs/AD1091750.pdf

As três arquiteturas que foram apresentadas nas imagens anteriores têm como objetivo apoiar uma estrutura de rede em malha, onde o tráfego pode fluir diretamente entre unidades ou nações nos escalões mais baixos, ao contrário de uma estrutura de rede em árvore ou stub, como é o caso dos escalões de comando mais elevados. Esta estrutura em malha é a topologia mais complexa, mas também a mais flexível e robusta e é utilizada maioritariamente nas unidades de escalões mais baixos, o que representa um desafio adicional às comunicações de cariz tático.

A figura abaixo mostra a conjunção das arquiteturas apresentadas anteriormente aplicadas a um cenário operacional da interligação entre duas unidades de escalão Companhia, dispondo de diferentes tipos de protocolos de roteamento e diferentes tecnologias.

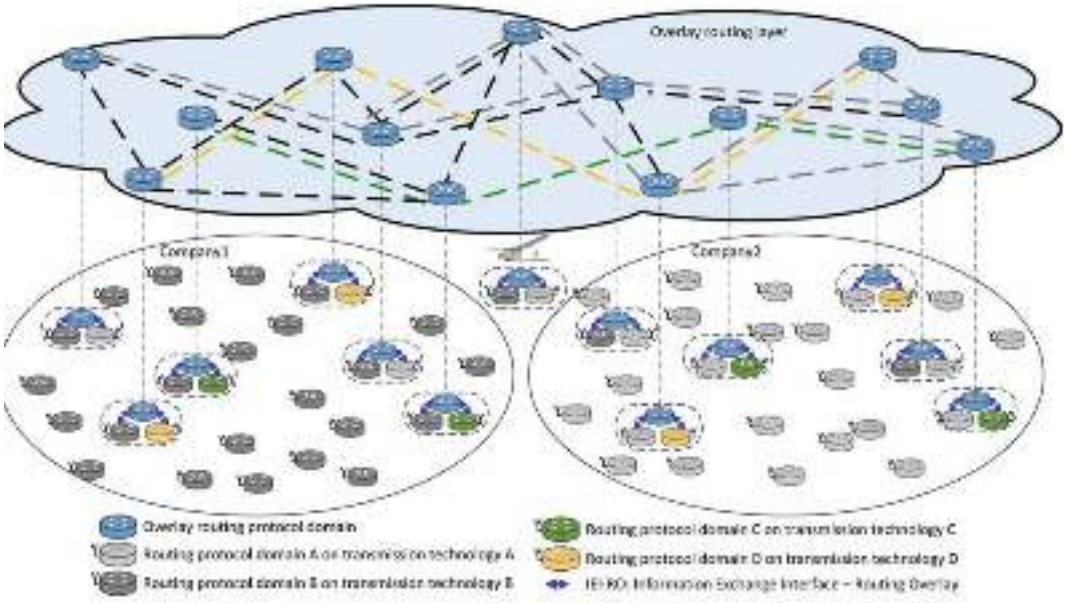


Figura 6 - Fonte: https://apps.dtic.mil/sti/pdfs/AD1091750.pdf

Importa referir que à data de hoje continua a ser difícil afirmar-se a existência de uma única arquitetura que se ajuste a todos os cenários, devido à sua elevada complexidade e diversidade de tecnologias e soluções utilizados pelos diversos países e forças armadas. Como tal, é relevante que se compreenda as características das diferentes arquiteturas e que se opte por implementar aquela (ou combinação de várias) que melhor se adapte à operação em particular.

Na figura seguinte é apresentada uma aproximação, em que são utilizados rádios com e sem cripto, na mesma plataforma (e.g. viatura de combate), tendo estes a possibilidade de garantir a interligação de voz e dados entre várias famílias de rádios e outros utilizadores que disponham de meios CSI em ambiente classificado e não classificado, respetivamente, não havendo interligação direta e funcional entre ambos.

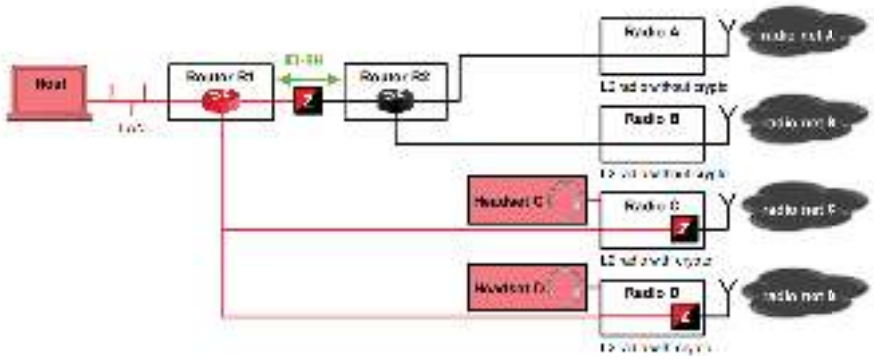


Figura 7 - Fonte: https://apps.dtic.mil/sti/pdfs/AD1091750.pdf

Para que qualquer uma das arquiteturas garanta a conectividade entre todos os seus elementos, deve ser possível estabelecer uma ou mais ligações entre diferentes forças e/ou nações. As abordagens possíveis para o estabelecimento destas ligações são as seguintes

• Utilizar uma tecnologia de transmissão padronizada pela NATO e que seja comum a alguns ou todos os parceiros, por exemplo, STANAG 5630 *Narrowband Waveform for VHF/UHF Radios* (NBWF);

• Utilizar uma tecnologia de transmissão proprietária comum a alguns ou todos os parceiros (por exemplo, rádio *Harris* 117G);

• Trocar alguns rádios nacionais (tecnologia de transmissão) com os parceiros;

• Roteamento através da malha de comunicações implementada com recurso a módulos de comunicações com capacidades acrescidas, em contexto de redes federadas com base na *framework FMN*.

Deste modo, prevê-se que uma combinação destas possibilidades poderá ser utilizada em contexto operacional, permitindo deste modo ultrapassar grande parte das dificuldades ao nível da interoperabilidade.

Coalition Waveforms (CWFs): A Chave para a Interoperabilidade

Neste seguimento, no âmbito da interoperabilidade das redes táticas heterogêneas, as *Coalition Waveforms (CWFs)* assumem um papel cada vez mais fundamental, pois estas formas de onda são desenhadas e especificadas com vista a garantir que os diversos sistemas de comunicações (hardware) dos diferentes países membros da NATO possam comunicar entre si, sem terem a necessidade de implementar alterações estruturais nos seus sistemas de comunicações já existentes, desde que estes já sejam disponham da funcionalidade de SDR[12] e na maioria dos casos que a sua tecnologia seja compatível com a *framework* SCA[13] de última geração.

[12] **SDR** – *Software Defined Radio*
[13] **SCA** – *Software Communications Architecture*

Tendo em conta as especificações do serviço *Communications Transport da FMN Spiral 5* e *6*, verifica-se a introdução de uma série de perfis e normativos que deverão ser tidos em conta na implementação de capacidades futuras de HTNs e CWFs, quer a nível nacional mas também por todos os afiliados. Cada mecanismo de troca de informação designa-se por *Technology Interactions (TINs)* a partir da *Spiral 5*, estando definidos um conjunto de perfis ou *standards* que podem ser utilizados pelos afiliados em cada uma dessas interações, a fim de garantir a sua interoperabilidade. A tabela seguinte resume o tipo de TINs que estão previstas neste serviço, bem como os perfis e *standards* que se prevê implementar em cada uma delas:

Technology Interaction	Profiles
Direct Cable Interconnection	• Inter-Autonomous Systems IP Transport Profile
Classified Local Area Network	• Inter Autonomous Systems IP Transport Profile
Public Network Transport Service	• IPv6 Transport Services Profile • Inter-Autonomous Systems IP Transport Profile • IPv4 Transport Services Profile
Military Network Transport Service	• Inter-Autonomous Systems IP Transport Profile • IPv4 Transport Services Profile • IPv6 Transport Services Profile
Information exchange over NBWF (Profile A)	• NATO Narrowband Waveform - Fixed Frequency (Edition 1)
Voice Exchange over SATURN with Legacy Crypto	• SATURN Secure Voice (Legacy)
Voice Exchange over SATURN with Modernized Crypto	• SATURN Secure Voice (STaC-IS)
Information exchange over NBWF (Profiles B and C)	• NATO Narrowband Waveform - Fixed Frequency (Edition 1)
Information exchange over NBWF EPM (Profile A)	• NATO Narrowband Waveform - Frequency Hopping (Edition 2)
Information exchange over NHDRWF	• NATO HDRWF (ESSOR) Standards Profile edition 1
Information exchange over IMT	• IMT Profiles (e.g. 3GPP specifications)
IMT Inter Tactical Bubble connectivity	• Not yet defined
IMT Tactical Radio Gateway	• Not yet defined
B.2 – ZT ISP Access Point automatized	• IPv4 Transport Services Profile • IPv6 Transport Services Profile • SMDP DP + Interfaces profiles • VPN Virtual Private Network • IP Quality of Service Profile
Voice exchange over TACSAT IW with Legacy Crypto	• UHF TACSAT Secure Voice (Legacy)
Voice exchange over TACSAT IW with Modernized Crypto	• UHF TACSAT Secure Voice (STaC-IS)
Data exchange over TACSAT IW with Modernized Crypto	• UHF TACSAT Secure Data (TSVCIS/LEFCIS/STaC-IS)
Voice exchange over HF with Modernized Crypto	• HF Secure Voice over Single-tone Narrowband Waveform
Information exchange over WB EPM SATCOM	• NATO Wideband SATCOM with EPM

(adaptado de *Communications Transport Service Instructions* – FMN *Spiral* 5 e 6)

Um aspeto relevante nestas especificações é que na maioria dos casos de uso das diversas TINs, exceto alguns casos pontuais, verifica-se na maioria dos casos um requisito de que a troca de informação estabelecida entre afiliados na *Tactical Coalition Radio Network* não deverá ser ter classificação de segurança superior a *NATO Restriced*, ou equivalente.

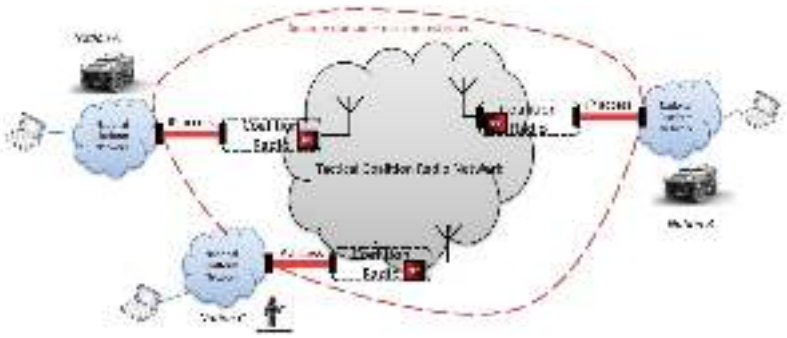


Figura 8 - HTNs e CWs implementadas em contexto operacional em termos das operações multi-domínio, aplicado ao âmbito do *Tactical Edge.*
Fonte: *Communications Transport Service Instructions – FMN Spiral 5*

Em termos práticos, as alterações estruturais no projeto TDCIS, nomeadamente a inclusão de uma *Coloured Cloud* adicional de classificação *Mission/National Restricted* faz todo o sentido, na medida em que a solução nacional estará alinhada com aquilo que a NATO prevê para o futuro neste contexto da implementação de sistemas CSI do *Tactical Edge*.

Outros projetos do Exército que contemplam a aquisição de rádios táticos, tais como o projeto C4I, CNR, entre outros, estão de igual modo adaptados a esta visão futura, na medida em que os rádios adquiridos (e.g. SOVERON SDTR VR5000 – Rádio de Banda Larga, HR5000 – Rádio de Baixos Escalões e P/PRC-525) têm a possibilidade de serem alvo de processo de acreditação para a classificação de segurança e marca de Nacional Reservado, uma vez que os modelos equivalentes destes rádios fabricados pela empresa Rohde & Schwarz (R&S) já foram certificados para *NATO Restricted*.

Desafios futuros na Implementação de HTNs e CWFs

Apesar de suas vantagens, a implementação das HTNs e CWFs apresenta desafios significativos, nomeadamente:

1. **Diversidade Tecnológica:** As forças da NATO usam uma variedade de sistemas, de diferentes épocas e capacidades. A integração de tecnologias tão distintas pode gerar problemas de compatibilidade e desempenho.

2. **Atualizações e Manutenção:** À medida que novas tecnologias surgem, as CWFs precisam ser atualizadas para garantir que continuem a funcionar com os novos sistemas. Isso requer testes rigorosos e investimentos contínuos em pesquisa e desenvolvimento.

3. **Gestão de Rede:** Gerir uma rede tática heterogénea envolve coordenar múltiplos sistemas em ambientes altamente dinâmicos, o que pode ser uma tarefa bastante complexa. A rede precisa ser monitorizada constantemente para garantir a sua eficiência e para identificar falhas rapidamente e atuar para as corrigir.

O futuro das HTNs e *Coalition Waveforms* parece promissor. Com o avanço das tecnologias de 5G, inteligência artificial e satélites de órbita baixa, é possível que as capacidades dessas redes e *waveforms* se expanda de forma significativa.

Espera-se que as futuras versões das CWFs possam lidar com uma maior largura de banda, maior segurança e maior eficiência na troca de dados em tempo real.

Além disso, a automação no processo de gestão das redes e o uso de inteligência artificial para otimizar as comunicações poderão tornar as operações da NATO ainda mais eficientes, permitindo uma melhor alocação de recursos e uma resposta mais rápida a falhas ou mudanças no ambiente envolvente do campo de batalha.

Por outro lado, embora grande parte dos cenários possam estar vinculados ao emprego de forças da componente terrestre, o conceito HTN e CFWs aplica-se praticamente a todos os domínios, com foco nos domínios tradicionais *Land, Maritime e Air,* mas com especial relevância no domínio *Space*, na medida em que esta tecnologia pode ser utilizada por sistemas de comunicações transversais a qualquer tipologia de força que participe em operações multi-domínio.

A figura seguinte mostra um exemplo visual de como cada vez mais é importante garantir a integração de todas estas componentes, para o qual o conceito HTN e CW representam um papel central e de extrema relevância.

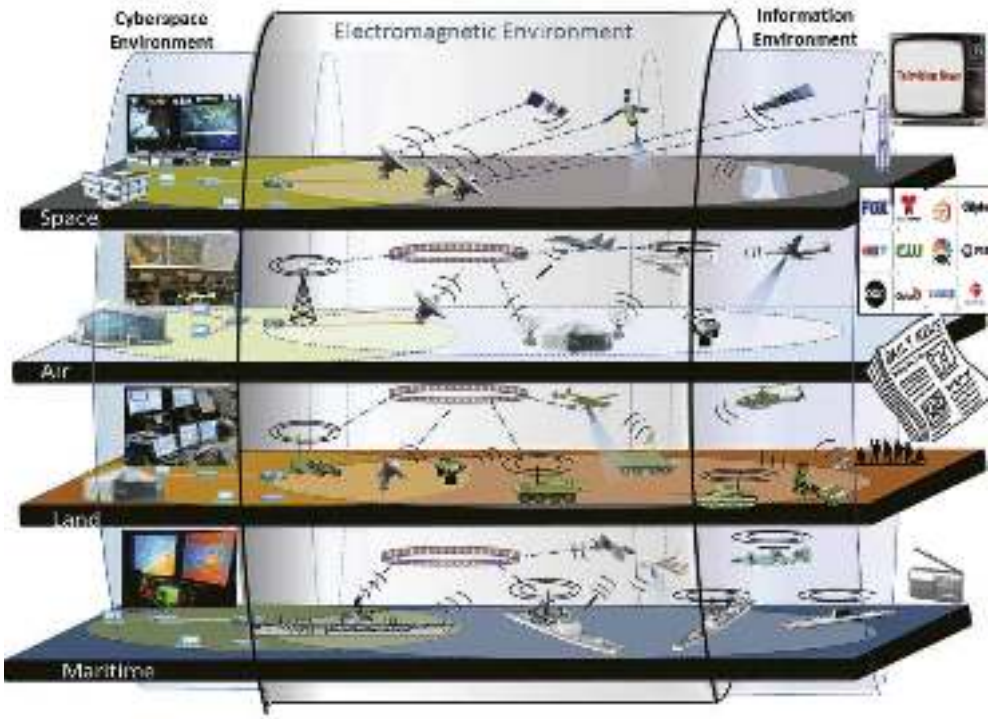


Figura 9 - Operações Multi-Domínio em todo o espetro eletromagnético.
Fonte: https://www.japcc.org/articles/electronic-warfare-the-forgotten-discipline/

Conclusão

As HTNs e as CWFs desempenham um papel essencial nas operações militares da NATO, especialmente quando se trata de garantir a interoperabilidade entre as forças aliadas. As CWFs, ao padronizar as comunicações entre diferentes sistemas, permitem que as forças de diferentes países operem de forma coordenada e eficiente, mesmo em ambientes desafiadores. A evolução das tecnologias de comunicação e a contínua inovação nas CWFs prometem aumentar ainda mais a flexibilidade, segurança e eficácia das redes táticas no futuro, garantindo que as forças da NATO possam manter sua superioridade em qualquer operação conjunta. Por este motivo, é relevante que Portugal e em particular o Exército Português continue a procurar acompanhar a evolução destes conceitos, materializando-os sempre que possível nos diversos projetos previstos relacionados com esta temática, como será o caso do já previsto *Mid-Life Upgrade* das viaturas PANDUR II, ou quaisquer outras viaturas de combate que sejam atualizadas e/ou adquiridas no futuro, bem como obviamente o projeto SIC-T /TDCIS, que é estruturante neste contexto.

Resumo da atividade do ano de 2024

Tenente-Coronel Tm Sílvia Gomes
Chefe da Secção de Operações Informações e Segurança do RTm

Durante o ano de 2024 o Regimento de Transmissões (RTm), fiel à sua missão e valores, continuou a afirmar-se como uma Unidade de referência no seio do Exército Português. O Batalhão de Transmissões (BTm) e a Companhia de Guerra Eletrónica (CompGE), encargos operacionais do Regimento, participaram em diversos exercícios nacionais e internacionais, tendo sido também realizado o aprontamento, com rotações semestrais, dos diversos Módulos de Comunicações e Sistemas de Informação (CSI) que integram as Forças Nacionais Destacadas para a República Centro Africana e para a Roménia. Durante este ano iniciou-se também o aprontamento da Companhia de Transmissões que integra o *European Union Battlegroup* 25-2/26-1 (EU BG 25-2/26-1).

Como Pólo de Formação da Escola das Armas o RTm ministrou 36 cursos, que corresponderam a 563 dias úteis de formação e 3642 tempos de formação. Estes cursos foram frequentados por 52 Oficiais, 116 sargentos, 182 Praças e 05 Civis.

Durante o ano transato, foram realizadas várias cerimónias militares e visitas de entidades militares e civis ao RTm. Destaca-se a visita de trabalho, em 01 de março, de Sua Excelência a Ministra da Defesa Nacional, Professora Doutora Helena Carreiras, tendo o RTm sido palco para a apresentação da capacidade de Comando e Controlo Terrestre do Exército. Houve ainda lugar às comemorações do Dia da Arma de Transmissões e do Regimento de Transmissões, em 3 de abril, o Juramento de Fidelidade de Oficiais, Sargento e Praças recém ingressados no Quadro Permanente, as visitas do Exmo TGen Comandante das Forças Terrestres e a Tomada de Posse do Comandante do RTm, a 12 de novembro. Em 2024 o Regimento teve ainda a honra de promover duas Cerimónias de Condecoração de Ex-combatentes do Ultramar, homenageando todos os que prestaram serviço em tempos de guerra, reconhecendo o seu sacrifício e dedicação.

Figura 1 – Cerimónia militar do Dia da Arma de Transmissões e do Regimento de Transmissões, em 03Abr24

Numa Unidade com um forte empenhamento em tarefas de Apoio de Área, mantivemos as portas abertas a entidades civis, instituições e escolas do distrito do Porto. Estas parcerias, que para o Exército potenciam as ações de divulgação do serviço militar entre os mais novos, da nossa história e cultura, permitem, por outro lado, e em determinada medida, colmatar uma necessidade das escolas e entidades civis em criar atividades e mecanismos de desenvolvimento de valores como a entreajuda, a solidariedade e o espírito de equipa.

O Centro de Divulgação do Dia da Defesa Nacional, sediado no RTm, recebeu a 20ª Edição durante 45 dias úteis, de 16 de janeiro a 20 de março, tendo comparecido 5908 jovens residentes nos concelhos do Porto, Maia, Matosinhos e Valongo.

No âmbito da iniciativa "Militar por um dia", desenvolvida pelo Exército, em abril a Unidade acolheu 19 alunos de escolas dos municípios de Lousada e Paços de Ferreira. Esta iniciativa tem como principal objetivo transmitir os valores da Instituição Militar e da cidadania, e envolver os jovens, durante 24 horas, em atividades de caráter essencialmente prático de natureza militar, promovendo a sua identificação com as Forças Armadas.

Figura 2 – Iniciativa "Militar por um Dia"

No ano em que se comemoraram os 50 anos do 25 de Abril de 1974, o Regimento recebeu centenas de jovens e alunos de várias escolas,proporcionando-lhes a oportunidade de conhecer uma Unidade Militar e alguns dos valores que partilhamos. Ainda no âmbito destas celebrações, o RTm realizou, no dia 24 de abril, uma Cerimónia de Hastear da Bandeira Nacional perante 1200 alunos do Colégio Luso-Francês, no Porto, associou-se à exposição de rádios da época promovida pela Associação de Radioamadores da Região de Lisboa e cedeu meios rádio da época para exposições em escolas da região do Porto. Além disso, o RTm apoiou a produção da série para a RTP1 "Daqui Houve Resistência", cedendo instalações para a realização de filmagens e reforçando a ligação entre o Exército e a cultura nacional.

Figura 3 – Cerimónia de hastear da Bandeira Nacional no Colégio Luso Francês, em 24Abr24

Além da sua ação em missões operacionais e de apoio à população, o Regimento esteve envolvido em diversas campanhas de solidariedade, destacando-se as ações de dádiva de sangue em parceria com o Instituto Português do Sangue e da Transplantação, com três campanhas realizadas ao longo do ano. Este gesto de generosidade foi mais uma demonstração da capacidade do RTm estar ao serviço da sociedade.

Em setembro o RTm organizou, no Parque da Cidade do Porto, o Campeonato Desportivo Militar de Corta-Mato Fase II, Comando das Forças Terrestres e Estrutura Superior do Exército, ao qual foi aberta a participação às Forças e Serviços de Segurança e ao Regimento de Sapadores Bombeiros do Porto, e que se materializou num salutar momento de convívio entre participantes e instituições. Para além disso, o Regimento participou na quase totalidade dos Campeonatos Desportivos Militares, nas suas diferentes Fases. Individualmente alcançaram-se resultados muito prestigiantes, quer ao nível do Exército e quer das Forças Armadas, dignificando o nome deste Regimento e dos militares de Transmissões.

No âmbito do apoio à proteção e salvaguarda de pessoas e bens, o RTm participou, durante os meses de julho, agosto e setembro, em diversas ações de vigilância dissuasora, em apoio da Autoridade Nacional de Emergência e Proteção Civil (ANEPC), da Guarda Nacional Republicana (GNR) e do Instituto da Conservação da Natureza e das Florestas (ICNF).

No que concerne ao Protocolo Faunos, estabelecido entre as Forças Armadas e o ICNF, foram realizadas 82 patrulhas de vigilância e dissuasão, num total de 41 dias de empenhamento, com 3 militares empenhados em cada patrulha e 9678 km percorridos na região de Vila Real.

No âmbito do Plano Hefesto II, que visa o apoio ao combate no âmbito do Sistema Integrado de Gestão dos Fogos Rurais, foi empenhado, no mês de setembro, o Representante das Forças Armadas na Sub-região do Tâmega e Sousa durante 4 dias em apoio desse Comanda Sub-regional da ANEPC, num dos períodos mais críticos de incêndios rurais vividos em Portugal no passado recente.

No que diz respeito ao Plano *Revelles*, que visa a vigilância e deteção no âmbito do Sistema Integrado de Gestão dos Fogos Rurais, em apoio da ANEPC e da GNR, foram realizadas 2 patrulhas de vigilância e deteção, num total de 2 dias de empenhamento, com 2 militares empenhados em cada patrulha e 911 km percorridos nas regiões de Vinhais e Carrazeda de Ansiães.

Em síntese, 2024 foi um ano de grandes realizações para o Regimento de Transmissões, que soube cumprir com distinção as suas missões operacionais e de formação, mantendo um compromisso inabalável com a proteção civil, a promoção da cultura militar, a solidariedade e a educação, o que se constrói, dia-a-dia, com a dedicação e o profissionalismo dos militares e civis que prestam serviço neste Regimento, fazendo "Sempre Melhor".

Figura 4 – Visita de crianças ao Regimento de Transmissões

Figura 5 – Campeonato Desportivo Militar de Corta-Mato Fase II CFT e Estrutra Superior do Exercíto, com a participação de entidades do Municipio do Porto

Arma de Transmissões - Dados estatísticos relativos ao ano de 2024

Capitão Tm Igor Pereira
Chefe da Secção de Pessoal do RTm, em suplência

Embora as mudanças na situação do Pessoal sejam, em geral, de conhecimento coletivo, é natural que prestemos mais atenção às alterações que envolvem os membros da nossa Arma. O presente artigo reúne informações sobre os Oficiais, Sargentos e Praças do Quadro Permanente da Arma de Transmissões que, no ano de 2024, tiveram a sua situação alterada, especialmente no que se refere a:

- Ingressos no Quadro Permanente
- Promoções/Graduações
- Passagens à situação de Reserva
- Passagens à situação de Reforma
- Abate ao Quadro Permanente
- Óbitos

1. INGRESSO NOS QUADROS PERMANENTES

a. Oficiais

Posto	NIM	Nome
Ten	00653619	Daniel Sampaio dos Reis Almeida
Ten	09911619	Ricardo Figueiredo Ferreira

b. Sargentos

Posto	NIM	Nome
2Sarg	11442216	Bruno Nóbrega do Patrocínio
2Sarg	09645120	José Duarte Baltar Leal
2Sarg	12457916	Miguel Duarte Gonçalves Fontoura
2Sarg	15514421	Rafael Pereira Marques Dias
2Sarg	08250822	José Carlos Gomes da Silva

c. Praças

Posto	NIM	Nome
CbAdj	09817917	Vânia Patrícia Guimarães do Carmo
CbAdj	12550002	Carlos Daniel Pinto Alves
CbAdj	11897312	Carlos Marcelo da Silva e Mota
CbAdj	17173517	António Manuel Arcanjo da Graça Carvalho
CbAdj	17167023	Alexandre dos Santos Carvalho
CbAdj	00810117	Ricardo José da Silva Crespo
CbAdj	12918516	Paulo Alexandre Carvalho Oliveira Moura
CbAdj	19557310	Ricardo Fernando Gomes da Mota

CbAdj	02024918	Joel André Ribeiro Teixeira
CbAdj	07164813	Tiago Alexandre Martins Pascoal
CbAdj	02345210	Ricardo Daniel da Hortinha Mocho
CbAdj	08353305	António Bernardo Rodrigues Vicente
CbAdj	14041719	António Paulo Cascalho de Oliveira

2. PROMOÇÕES

a. Oficiais

(1) Quadro Especial de Transmissões

Posto	NIM	Nome
Cor	36287892	Paulo Sérgio Madaleno Soares
Cor	02140689	Alberto Lopes Correia
Cor	15182893	João Francisco Branco Barreira
Cor	29948991	Fernando António Antunes da Silva
TCor	04224400	Sílvia Andrea Teixeira Gomes
Maj	02550006	Gonçalo Correia Soeiro
Maj	14955306	Luís Filipe Fonseca Regada
Maj	15188306	Francisco Domingues Jorge
Maj	07001809	Filipe Alexandre Valdeira João
Maj	15371906	Tiago Daniel Sanches de Almeida
Maj	02523106	Renato Gonçalves Rocha
Cap	17555415	Simão Pedro Avelino Valente
Cap	12553815	Pedro Miguel Martins Leitão da Costa

(2) Quadro Especial de Técnicos de Exploração de Transmissões

Posto	NIM	Nome
TCor	12986491	Paulo Jorge Martins da Silva
TCor	12393888	José Luís Mendes Torres

(3) Quadro Especial de Técnicos de Manutenção de Transmissões

Posto	NIM	Nome
TCor	06954488	Augusto Manuel Andrade Santos

b. Sargentos

(1) Quadro Especial de Transmissões

Posto	NIM	Nome
SMor	10565888	Jorge Emídio Simões da Cruz
SMor	00634988	Paulo José Freitas Fiel
SMor	12593889	Artur Jorge Neves Pinto
SMor	09838588	Eurico de Jesus Rebelo
SMor	09804889	Paulo Jorge Barroso Martins
SMor	02381989	Paulo Jorge Martins da Costa
SMor	16032989	Jorge Manuel Lima da Silva Rocha
SCh	12115393	Elvira Gabriela F. Fernandes Moura
SCh	15060393	João Pedro Fernandes Mouta
SCh	28419793	Arsénio Manuel Bernardino Moço
SCh	10342595	Jacinto Marques das Neves
SCh	05154995	Pedro Manuel Silva Soares
SCh	05925495	Fernando Manuel Rebelo Duarte
SCh	00753991	Teresa Maria Silvestre Lamas
SCh	28939891	Francisco José de Passos C. Paínhas
SCh	31754893	João Paulo Pires Marques
SCh	23463192	Noémia Delfina Martins Nunes Magalhães
SCh	28986893	Joaquim Rebelo Torres
SCh	34233293	Luís Filipe Guerreiro Ledo
SCh	16004094	Marco António Mendes de Melo
SCh	06014094	Paulo Alexandre Pinto Nogueira
SCh	23260892	Nuno Miguel Mendes Cardoso Ferreira
SAj	00157606	Nélson Simplício André Pinho
SAj	18734610	Carlos Miguel Sá de Carvalho
SAj	01291809	André Pereira Barbosa
SAj	11822605	Christopher Manuel Alves Monteiro
SAj	08835301	António Luís Pinto Carvalho
SAj	13279904	André Filipe Alves da Costa Marques
SAj	04503909	Suzana Dalila Alomaya Tavares
SAj	14292206	Wilson Filipe Pinto Cardoso
SAj	07758904	Rúben Rodrigues Bota
SAj	00176704	Ricardo Miguel Ramalho Pestana Fialho

SAj	19909005	Adam Gregory Lambert
SAj	14348500	Vítor José Vieira Santos
SAj	04999905	Vítor Joel Crespo dos Santos
SAj	16649206	Ricardo Jorge Pereira Loureiro dos Santos
SAj	04247103	Eugénio Rogério Henriques Fragoeiro
SAj	06700905	Hélder Manuel da Costa Soares
SAj	03914306	Fábio Vila Pires
SAj	08114806	Andreia Libânia Pinto de Sousa Nascimento
SAj	13386704	Paulo Renato Aveiro de Viveiros
SAj	15635806	Tiago Alexandre Cavaleiro Ferreira
SAj	04540006	Miguel da Silva Filipe
SAj	12074905	Hélder Filipe Fernandes Monteiro
SAj	19662306	João Pedro Batista Rocha
1Sarg	06141614	Inês Isabel Perdigão Mendes
1Sarg	10754117	Fábio Rafael Rodrigues Amaral
1Sarg	00352215	Tiago Alexandre Casadinho Leonor
1Sarg	07291015	Tiago Filipe Pereira Miranda
1Sarg	16186312	Rodolfo Alves Oliveira
1Sarg	09138818	Francisco Manuel Ramalho Luzio
1Sarg	14994114	Raphael Antony Ferreira

3. PASSAGEM À SITUAÇÃO DE RESERVA

a. Oficiais

Posto	NIM	QEsp	Nome
Cor	18941587	Tm	José António da Silva Vieira
Cor	16216989	Tm	Joaquim Fernando de Sousa Ferreira
Cor	04138589	Tm	António Pedro Velez Quaresma Rosa
Cor	14260990	Tm	António Martins Limão de Oliveira Jarmela
Cor	08204589	Tm	João Manuel Fernandes Correia
TCor	08233988	Tm	Alexandre Miguel Gil Fernandes
TCor	11669386	TExpTm	João Manuel Guerra Batista
TCor	10789787	TManTm	Carlos Manuel Martins Prada
TCor	12393888	TExpTm	José Luís Mendes Torres
TCor	06954488	TManTm	Augusto Manuel Andrade Santos

b. Sargentos

Posto	NIM	QEsp	Nome
SMor	08896285	Tm	Eusébio Fernandes Ferreira
SMor	07048887	Tm	Arnaldo Paulo Silva Pereira
SMor	15023787	Tm	António Armando Senane Custódio
SMor	00634988	Tm	Paulo José Freitas Fiel
SCh	15270188	Tm	Vítor Manuel dos Santos Esteves
SCh	03787990	Tm	Reinaldo Alexandre Martins dos Santos Pires
SCh	12776590	Tm	José Manuel de Oliveira Gonçalves
SCh	01912289	Tm	Jorge Manuel Tiago Vieira

4. PASSAGEM À SITUAÇÃO DE REFORMA

a. Oficiais

Posto	NIM	QEsp	Nome
TCor	09696279	TManTm	José Manuel Girão Lima
TCor	07562779	TManTm	Fernando de Freitas Lúcio

b. Sargentos

Posto	NIM	QEsp	Nome
SMor	06453683	Tm	António Luís Paiva Madail
SMor	14566481	Tm	Vítor Manuel Reis Mineiro
SMor	18432880	Tm	Fernando Rodrigues Ferreira
SMor	05342780	Tm	Francisco dos Anjos Luís
SCh	02380586	Tm	Luís Veiga Maria Loureiro

5. ABATE AO QUADRO PERMANENTE

a. Oficiais

Posto	NIM	QEsp	Nome
Cap	11476612	Tm	Fernando Augusto da Costa Batista
Cap	15283213	Tm	Kevin Correia Lourenço

6. ÓBITOS

Posto	NIM	QEsp	Nome	Data Falecimento
Cap	51778711	Tm	António Castiço Antunes Guerra	06JAN24
TCor	06226390	Tm	Carlos Manuel Machado Grilo	14JAN24
Cor	50772611	Tm	Francisco António Frade	22JAN24
SCh	32258059	Tm	José da Costa	31JAN24
SMor	04252784	Tm	Mário António Rodrigues Correia Pereira	02FEV24
SAj	12715289	Tm	Mário Jorge Santana Ferreira	01MAR24
Maj	51065911	Tm	Francisco José Gil	05MAR24
Maj	52398211	Tm	Zeferino Manuel Rodrigues Moreira	07MAR24
TCor	51689111	Tm	Vítor Manuel Correia Santos	02ABR24
CbAdj	42048655	Tm	Manuel Simões Gouveia	03MAI24
1Sarg	50209711	Tm	Manuel Esteves	16MAI24
Cap	51055811	Tm	Fernando Gomes da Palma	10JUN24
Cap	52403411	Tm	José Augusto Ribeiro Barros	14JUN24
SAj	02515278	Tm	Francisco Manuel Semião Pinto	13AGO24
SCh	51717911	Tm	José Correia de Figueiredo	19AGO24
Cor	50767411	Tm	Carlos Alberto Borges do Rego Falcão	09NOV24
2Sarg	51048111	Tm	António Silva Mendes	26NOV24
SMor	03805175	Tm	Eduardo Jorge Barbosa Miranda	27NOV24
SMor	01516363	Tm	Fernando Rodrigo Rosa Couto	02DEZ24

A Formação no Regimento de Transmissões

Major Tm Martingo Coelho
Chefe da Secção de Formação do RTm

A formação no Regimento de Transmissões (RTm), encontra-se organizada em diferentes áreas: Redes de Computadores (Academia Cisco), Aplicações e Sistemas de Informação (Academia Microsoft), Comunicações Rádio e C2, Guerra Eletrónica (GE), Material e Segurança Cripto, sendo ainda ministrados cursos de "Instrução Complementar Específica de Transmissões - Praças" e cursos de Promoção a Cabo.

A rápida evolução tecnológica, associada ao aumento da complexidade dos Sistemas de Informação e Comunicações, implicam uma atualização frequente da formação de Comunicações e Sistemas de Informação (CSI), para uma adequada preparação dos militares e civis para a operação, configuração e gestão dos respetivos sistemas e equipamentos. Neste âmbito, durante o ano de 2024 foram implementados e aprovados os seguintes cursos/formações:

- Configuração e Gestão do *Battlefield Management System* (BMS);
- Microsoft *Sharepoint*;
- UFCD E01845A - Hardware de Computadores;
- UFCD E01844A - Sistema Operativo Cliente.

Figura 1 - Curso Microsoft *Sharepoint*

A Academia Cisco e a Academia Microsoft, implementadas no RTm, permitem que sejam ministradas formações de elevada qualidade, com reconhecimento e certificação internacional, garantindo simultaneamente o acompanhamento da evolução do conhecimento técnico através da atualização dos currículos dos cursos de forma frequente.

Ao longo do último ano, o Regimento de Transmissões ministrou os seguintes cursos/ formações:

• **IT-ESSENTIALS** o 1.ª Edição de 04Jan24 a 31Jan24; o 2.ª Edição de 26Fev24 a 22Mar24; o 3.ª Edição de 22Abr24 a 22Mai24; o 4.ª Edição de 14Out24 a 11Nov24.	• **CISCO CERTIFIED NETWORK ASSOCIATE - ROUTING&SWITCHING** o 1.ª Edição de 26Fev24 a 26Jun24 o 2.ª Edição de 06Mai24 a 01Ago24

• **CISCO CERTIFIED NETWORK ASSOCIATE – CYBERSECURITY OPERATIONS** o De 07Out24 a 02Dec24	• **CISCO CERTIFIED NETWORK ASSOCIATE - VOICE OVER INTERNET PROTOCOL** o 22Jan24 a 09Fev24
• **UFCD E01845A - HARDWARE DE COMPUTADORES** o 16Set24 a 20Set24	• **MICROSOFT TECHNOLOGY ASSOCIATE - WINDOWS SERVER** o 1.ª Edição de 02Abr24 a 02Mai24 o 2.ª Edição de 12Nov24 a 09Dec24
• **MICROSOFT SHAREPOINT** o 1.ª Edição de 22Jul24 a 26Jul24 o 2.ª Edição de 09Dec24 a 13Dec24	• **MATERIAL E SEGURANÇA CRIPTO – PRAÇAS** o 1.ª Edição de 19Fev24 a 23Fev24 o 2.ª Edição de 01Jul24 a 05Jul24 o 3.ª Edição de 09Set24 13Set24
• **MICROSOFT OFFICE SPECIALIST** o 1.ª Edição de 15Jan24 a 09Fev24 o 2.ª Edição de 30Set24 a 25Out24	• **UFCD E01844A - SISTEMA OPERATIVO CLIENTE** o 23Set24 a 27Set24
• **OPERAÇÃO DO SISTEMA P/525** o 1.ª Edição de 19Fev24 a 23Fev24 o 2.ª Edição de 15Abr24 a 19Abr24 o 3.ª Edição de 08Jul24 a 12Jul24 o 4.ª Edição de 18Nov24 a 22Nov24 o 5.ª Edição de 16Dec24 a 20Dec24	• **CONFIGURAÇÃO E GESTÃO DO SISTEMA P/525** o 1.ª Edição de 08Jan24 a 19Jan24 o 2.ª Edição de 02Set24 a 13Set24 o 3.ª Edição de 25Nov24 a 06Dec24
• **CONFIGURAÇÃO E GESTÃO DO BATTLEFIELD MANAGEMENT SYSTEM** o 1.ª Edição de 01Jul24 a 05Jul24 (Formação de Formadores) o 2.ª Edição de 17Jul24 a 30Jul24	• **FUNDAMENTOS E ESTRUTURA DE GUERRA ELETRÓNICA** o 05Fev24 a 09Fev24

• **OPERAÇÕES DE GUERRA ELETRÓNICA** o 07Out24 a 02Dec24	• **INSTRUÇÃO COMPLEMENTAR ESPECÍFICA DE TRANSMISSÕES – PRAÇAS** o 07Out24 a 16Out24
• **CURSO DE PROMOÇÃO A CABO** o 1.ª Edição de 19Fev24 a 01Mar24 o 2.ª Edição de 13Mai24 a 24Mai24 o 3.ª Edição de 01Set24 a 12Set24 o 4.ª Edição de 18Nov24 a 29Nov24	

Figura 2 - Curso de Configuração e Gestão do Sistema P/525

O RTm tem disponibilizado este tipo de formação não só a militares e civis do Exército, como também a militares e civis do Estado-Maior-General das Forças Armadas (EMGFA), Forças de Segurança, bem como a militares das Forças Armadas de outros países.

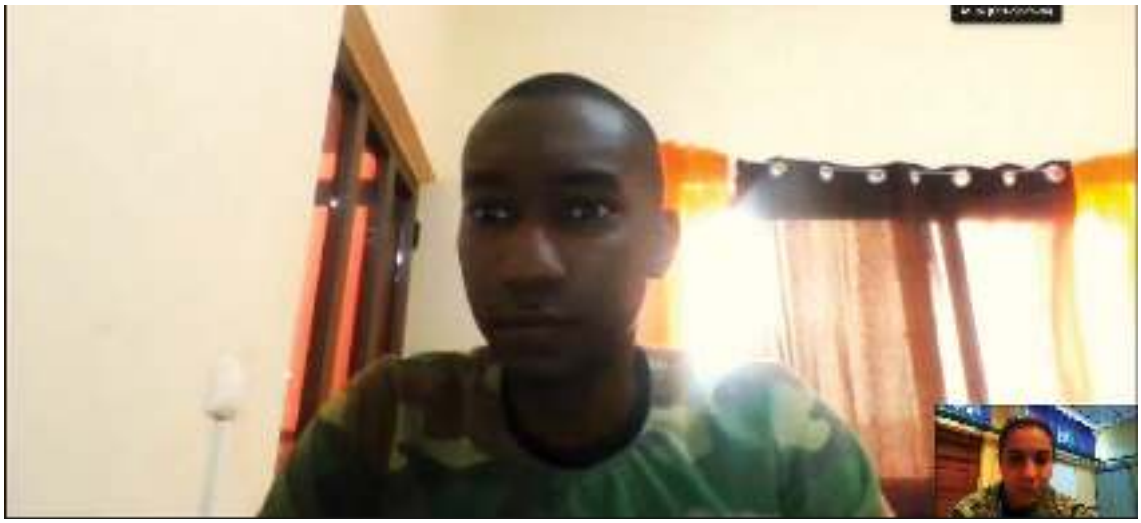


Figura 3 – Militar das Forças Armadas de Cabo Verde frequenta o curso *IT-Essentials* do RTm

Em 2024, um militar da República de Cabo Verde (cooperação no domínio da Defesa/Cooperação técnico militar com a República de Cabo Verde) frequentou com aproveitamento o curso "IT-Essentials" (04Jan24 a 31Jan24). De destacar ainda a frequência por parte de dois oficiais da Guarda Nacional Republicana (GNR) nos seguintes cursos: *IT-Essentials* (26Fev24 a 22Mar24), *Microsoft Technology Associate - Windows Server* (02Abr24 a 02Mai24) e *Cisco Certified Network Associate - Routing & Switching* (06Mai24 a 01Ago24).

O curso *Cisco Certified Network Associate – Cybersecurity Operations (CyberOps)* (07Out24 a 02Dec24), além de militares do Exército, contou também com a participação de militares do Comando de Operações de Ciberdefesa (COCiber) do Estado-Maior-General das Forças Armadas (EMGFA).

Figura 4 – Curso CCNA-CyberOps no RTm

A procura deste tipo de cursos por partes de entidades externas ao Exército, constituiu um sinal inequívoco do reconhecimento da qualidade da formação em CSI, ministrada pela Secção de Formação do Regimento de Transmissões.

Figura 5 – *Curso Voice Over Internet Protocol* (Esquerda) e Curso *IT-Essentials* (Direita)

No entanto, apesar do reconhecimento comprovado da qualidade da formação ministrada, a maioria dos equipamentos que constituem os laboratórios e salas de aulas encontram-se em fim de vida e desatualizados, face aos novos conteúdos ministrados. É imperativo a atualização dos equipamentos e recursos didáticos da Secção de Formação do Regimento de Transmissões, para que este continue a poder ministrar formação de qualidade, certificada e atualizada.

J6 Branch da EUTM MOZ e EUMAM MOZ

Major Tm Luís Regada
J6 Officer / CIS Security and Cyber Operations

A pedido do Governo moçambicano, a União Europeia (UE) estabeleceu a *European Union Training Mission in Mozambique* (EUTM MOZ) com um mandato não executivo, de 15 de outubro de 2021 até 31 de agosto de 2024. A EUTM MOZ teve como objetivo apoiar as Forças Armadas de Defesa de Moçambique (FADM), para dar resposta à crise em Cabo Delgado.

Através deste treino foram capacitadas 11 Forças de Reação Rápida (QRF), para que as FADM possam, de forma independente, desenvolver as capacidades necessárias e sustentáveis para restaurar a segurança e oferecer capacidade de proteção à população civil em Cabo Delgado. No total foram formados 1700 militares e 100 instrutores.

Na sequência dos resultados positivos da EUTM MOZ e da parceria militar de longa duração da UE com Moçambique surge a *European Union Military Assistance Mission in Mozambique* (EUMAM MOZ), sediada em Maputo. Com início a 1 de setembro de 2024, a EUMAM MOZ é uma continuação lógica da EUTM e tem como missão apoiar as QRF das FADM a atingir um ciclo operacional sustentável, em conformidade com o Direito Internacional Humanitário.

Figura 1 – EUTM MOZ logo

Figura 2 – EUMAM MOZ logo

Em ambas as missões, o *J6 Branch* integra o *Mission Force Headquarters* (MFHQ) estando na dependência direta do 2.º Comandante e Chefe de Estado-Maior. Este ramo é responsável por gerir e manter todos os Sistemas de Informação e Comunicações (SIC). Na EUTM MOZ, o *J6 Branch* era composto por cinco Elementos Nacionais Destacados (END), nomeadamente um Oficial Superior e quatro Sargentos, todos da Arma de Transmissões do Exército Português. Devido ao encerramento da posição de Chimoio e à redução de dois cargos de Sargento de Transmissões, na EUMAM MOZ, o *J6 Branch* passa a ser composto por 3 END.

O cargo de *J6 Officer / CIS Security and Cyber Operations* é garantido por um TCor/Maj em Maputo. Na EUTM MOZ, além de ser o principal responsável pelo *J6 Branch* tanto em Maputo como em Chimoio, tinha também a dupla função de *Trainer CIS Planning Cycle*. Na EUMAM MOZ é o responsável pelo *J6 Branch* e acumula com a função do extinto cargo *J3 Cyber OPS Officer* na coordenação das atividades de ciberdefesa.

Na EUTM MOZ em Chimoio, existiam duas funções para Sargentos de Transmissões (SCh/SAj/1Sarg/2Sarg), nomeadamente o cargo de *J6 CIS Specialist (Server / End User Assets Management)* que era responsável pelo apoio informático e de *helpdesk*, e o cargo de *S6 Head / Network* que além de apoio informático e de dirigir o apoio do CIS, tinha a dupla função de Formador de Comunicações. Estas duas funções deixaram de existir com o encerramento da posição em Chimoio após a transição para a EUMAM MOZ.

Tanto na EUTM MOZ como na EUMAM MOZ, sempre em Maputo, há duas funções para Sargentos de Transmissões (SCh/SAj/1Sarg/2Sarg), nomeadamente o cargo de J6 CIS NCO que além do apoio informático e de *helpdesk* é o responsável por todos os aspetos administrativos do J6 Branch, e o cargo de *J6 ComSec (Satcom / Network)* que presta apoio informático e de *helpdesk*, e é também o responsável pelos equipamentos criptográficos (tanto europeus como portugueses) e pelas comunicações satélites.

Figura 3 – *J6 Branch*

O maior desafio enfrentado pela 6ª (e última) rotação da EUTM MOZ, que foi também a 1ª rotação da EUMAM MOZ, foi a fase de transição entre as missões.

Com o encerramento da EUTM MOZ, encerrou também o campo de treino de Chimoio. Para o *J6 Branch* isto significou resolver todos os processos administrativos relativos a acertos de cargas, empacotar e transportar o material de Chimoio para Maputo e para alguns estados-membros da EU. Foi ainda necessário cancelar todos os contratos (internet fixa, comunicações móveis, serviço de impressão, videovigilância e controlo de acessos), realizar o *backup* da informação e desmontar toda a infraestrutura de rede (Classificada e Não Classificada).

Esta foi, sem dúvida, uma tarefa crítica que foi planeada e executada com sucesso. Para isso, foi essencial o profundo envolvimento, profissionalismo e enorme capacidade de trabalho dos *5 ENDs* da Arma de Transmissões, presentes em Moçambique à data da transição.

Na EUTM MOZ, entre outras tarefas, o J6 Branch otimizou a rede Não Classificada, especialmente o acesso à Internet, a partilha de ficheiros, a voz sobre IP (VoIP), a rede sem fios e o controlador de domínio, a manutenção do sistema de videoconferência, a rede rádio VHF, entre outras ferramentas essenciais para a elevada produtividade da missão.

Na procura das melhores soluções para os desafios das Comunicações e Sistemas de Informação (CSI) da EUMAM MOZ, competências como o profissionalismo, organização e experiência em Redes de Computadores, Segurança de Redes Informáticas, Administração de Sistemas e Tecnologias de Informação foram essenciais para a transição das missões. Nesta fase, o *J6 Branch* teve um papel fundamental, pois analisou o mercado e reviu todos os contratos à sua responsabilidade, nomeadamente as Comunicações Móveis, Televisão, Serviço de Impressão, *Internet Service Provider* (ISP), *Webex*, entre outros. Para além disso, reorganizou a rede EU RESTRICTED, assegurando a correta utilização dos sistemas de informação classificados, tanto os da EU como os portugueses.

Outra tarefa crítica, planeada e executada em paralelo com o encerramento de Chimoio, executada apenas com 3 ENDs em Maputo, foi a reestruturação da rede Não Classificada. Com isto criaram-se condições para um aumento da produtividade de toda a Missão, exponenciando a possibilidade de organização da informação e do trabalho colaborativo. Contribuiu para isto a formatação de cerca de 110 computadores e instalação do *Windows 11* nos mesmos, a implementação do *Microsoft 365* com *OneDrive*, *SharePoint* e *Teams*, a criação do novo Domínio de Email e a reconfiguração dos telefones VoIP, sendo esta implementação um salto tecnológico sem precedentes.

Figura 4 – *SharePoint* EUMAM MOZ

Integrar uma Força Multinacional Conjunta e Combinada da União Europeia que planeou e executou o encerramento de uma Missão e, em paralelo, planeou e executou a transição e posterior implementação de uma nova Missão, sendo responsável pelas Comunicações e Sistemas de Informação e Ciberdefesa (Chefe do J6), foi um privilégio e uma experiência extremamente desafiante, enriquecedora e única.

Esta experiência, com autonomia financeira e liberdade de ação na implementação das melhores soluções para os diversos desafios, permitiu-me desenvolver competências técnicas e de liderança, proporcionando-me uma compreensão mais profunda da importância da cooperação internacional e da resiliência em ambientes complexos, pelo que levo comigo lições valiosas que certamente aplicarei em futuras missões.

Figura 5 - Constituição do J6 EUMAM MOZ

O Papel da Ciberdefesa na segurança da missão da EUTM-Moçambique

Capitão Tm Pedro Marques
J3 Cyber Ops Officer /EUTM-MOZ RTm

Enquadramento

Devido ao agravamento da instabilidade securitária causada pelos ataques insurgentes na região de Cabo Delgado, em Moçambique, e à subsequente crise humanitária, o Conselho da União Europeia (UE) decidiu implementar uma missão não executiva, designada European Union Training Mission - Mozambique (EUTM-MOZ). Esta missão tem como objetivo apoiar as Forças Armadas e de Defesa de Moçambique (FADM) através da formação militar de 11 *Quick Reaction Forces* (QRFs), com o intuito de desenvolver capacidades sustentáveis para proteger a população civil e restaurar a segurança em Cabo Delgado, sempre em conformidade com os princípios do direito internacional humanitário e os direitos humanos[1].

A EUTM-MOZ é composta por militares e civis de países da UE, com efetivo máximo previsto de 120 pessoas, contando atualmente com a participação de 11 países (figura 1). Portugal, como membro da UE, contribui com 60 militares, provenientes dos três ramos das Forças Armadas. Além disso, Portugal é a Lead Nation, tendo assumido o comando da EUTM-MOZ em setembro de 2021.

Figura 1 – Países que atualmente representam a EUTM-MOZ

Arquitetura CSI na EUTM-MOZ

A fim de garantir o Comando e Controlo (C2) e proporcionar ao *Mission Force Commander* a liberdade de manobra na área de operações em Moçambique, foi implementada uma arquitetura de Comunicações e Sistemas de Informação (CSI), utilizando tecnologias de comunicações, por satélite, rádio móvel e fibra ótica, conforme é possível visualizar na figura 2. A ligação principal entre a EUTM-MOZ e o escalão superior, o *Military Planning and Conduct Capability* (MPCC), é estabelecida por meio de dois *links* satélite[2].

A nível operacional e tático, foi implementada uma rede IP não classificada entre o *Mission Force* (MF) *Headquarters* (HQ) Maputo e o HQ Chimoio, oferecendo serviços como *Internet, VoIP, File Share, Remote Authentication Dial In User Service* (RADIUS), Monitorização através do Zabbix, entre outros. A arquitetura CSI também inclui uma rede de rádio para comunicação entre os HQs e os Campos de Treino, com estações base interligadas por IP, permitindo a monitorização de rádios portáteis. Em situações mais complexas, como catástrofes naturais, a EUTM-MOZ utiliza telefones satélite e ligações satélite portáteis.

[1] Jornal Oficial da União Europeia, Decisão (PESC) 2021/1143 do Conselho de 12 de julho de 2021
[2] Implementação da Arquitetura CSI na EUTM-Moçambique [Artigo Maj Tm Fábio Silva]

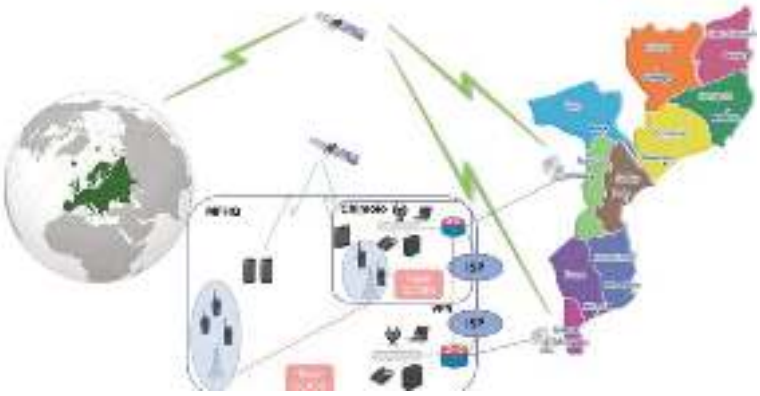


Figura 2 – Arquitetura CSI na EUTM-MOZ

O Papel do Oficial de Operações de Ciberdefesa na EUTM-MOZ

No âmbito da missão da EUTM-MOZ, a Ciberdefesa (CD) assume uma importância essencial, com a crescente sofisticação das ciberameaças no domínio do ciberespaço. Estas ameaças podem comprometer os objetivos da missão através do acesso indevido aos sistemas CSI e à segurança da informação. Por forma a mitigar as vulnerabilidades dos sistemas CSI e garantir a sua resiliência, foi implementada uma estrutura de CD. Esta estrutura é liderada pelo *J3 Cyber Ops* da EUTM-MOZ, cuja responsabilidade abrange a coordenação e liderança das atividades de ciberdefesa, garantindo que todos os riscos sejam tratados com a máxima seriedade. Além desta responsabilidade o *J3 Cyber Ops* tem como importantes contributos para a missão, os seguintes:

1. Liderar e gerir a estrutura de CD na missão da EUTM-MOZ, sendo responsável pela coordenação de todas as operações de CD;
2. Apoiar na implementação de medidas para prevenir, detetar e responder a incidentes de CD. Em caso de necessidade coordenar ações de recuperação, por forma a minimizar o impacto da ameaça;
3. Responsável pela monitorização continua do ciberespaço, fundamental para antecipar e mitigar riscos para a informação e sistemas CSI da missão.
4. Implementar e atualizar os *standards operating procedure* (sop) no domínio da CD, garantindo que todos os membros da missão sigam um conjunto claro de normas e práticas seguras;
5. Contribuir para consciencialização das ameaças existentes através da elaboração de um quadro semanal das ameaças CD bloqueadas pela estrutura de CD da missão.
6. Periodicamente, ou quando necessário, realizar ações de formação na área de CD, assegurando que todos os membros da missão recebem as competências necessárias para executar as melhores práticas no domínio do ciberespaço, mitigando dessa forma a exposição à ameaça.
7. Além das atividades dentro da missão, o *J3 Cyber Ops* apoia na formação de CD às FADM, contribuindo na capacitação e conhecimento técnico das FADM na área de CD.

Figura 3 – Imagem genérica alusiva à proteção da informação nos CSI

Conclusões

A EUTM-MOZ desempenha um papel fundamental na formação e fortificação das capacidades de defesa de Moçambique, com o objetivo de proteger a população civil e restaurar a segurança na província de Cabo Delgado.

No entanto, os objetivos da EUTM-MOZ para não serem comprometidos através das ciberameaças, existe a necessidade de estar implementada uma estrutura CD para proteger os sistemas CSI e garantir a integridade e confidencialidade da informação da EUTM-MOZ. A função de *J3 Cyber Ops*, desempenha uma função de extrema importância na coordenação e liderança dessa estrutura CD, através da implementação de medidas para prevenir, detetar e responder a ameaças do ciberespaço. A importância da função não fica só pela sua componente técnica de execução, mas também no apoio ao desenvolvimento da capacidade CD das FADM.

Figura 4 – Cerimónia em Parada na EUTM-MOZ (Maputo)

Bibliografia

[1] Jornal Oficial da União Europeia, Decisão (PESC) 2021/1143 do Conselho de 12 de julho de 2021;
[2] Implementação da Arquitetura CSI na EUTM-Moçambique [Artigo Maj Tm Fábio Silva].

Módulo de Comunicações na República Centro-Africana – 14ªFND/MINUSCA

Capitão Tm Jonathan Guimarães
Chefe do Módulo CSI da 14ª FND RCA

Desde janeiro de 2017 que Portugal participa, ativamente, na *Multidimensional Integrated United Nations Stabilization Mission in the Central African Republic* (MINUSCA) como *Quick Reaction Force* (QRF). É uma missão de elevado risco, onde a QRF portuguesa está à disposição do Force Commander da MINUSCA, Tenente-General Humphrey Nyone, para a empregar em qualquer zona do país.

A Missão

A Força Portuguesa tem como *Main Operational Base* (MOB) o Campo Portugal, integrado no campo *Greenfield*, onde estão aquarteladas múltiplas Forças da MINUSCA, em Bangui, capital da República Centro-Africana (RCA). É a partir desta MOB que a Força Nacional Destacada (FND) composta por 215 militares se prepara para ser empenhada em missões. Essa preparação passa pelo treino contínuo dos militares e pela preparação de todo o apoio de combate e de serviços, tal como as Comunicações e Sistemas de Informação (CSI).

A Missão do Módulo de Comunicações na MOB

O Módulo de Comunicações (ModCom) desta FND é composto por um Oficial, 4 Sargentos e 4 Praças. Para a 14ªFND/MINUSCA, que foi constituída maioritariamente por militares do Regimento de Infantaria nº10 (RI10), tendo como base o 2ºBatalhão de Infantaria Paraquedista, o Regimento de Transmissões (RTm) garantiu o grosso do ModCom, nomeadamente um Oficial, 3 Sargentos e 3 Praças, sendo que um Sargento foi proveniente do RI10 e uma Praça da Companhia de Transmissões da Brigada de Reação Rápida. A Força foi projetada para o Teatro de Operações (TO) a 4 de dezembro de 2023, tendo-se dado a retração em 5 de junho de 2024.

Na MOB, o ModCom faculta todos os recursos de CSI necessários para as operações e bem-estar. A estrutura implementada na MOB, baseia-se numa extensão do domínio do Sistema de Informação e Comunicações Operacional (SIC-Op) com a ligação ao Território Nacional (TN) garantida através de uma ligação satélite em banda X (Figura 1). Foi também implementada uma ligação de internet, assente numa estrutura civil em banda C (Figura 2), com uma largura de banda aproximada de 16 Mbps, usada sobretudo como internet de trabalho, ou seja, integrada com a Rede de Dados do Exército para toda a componente de planeamento e envio de relatórios da parte do Comando e Estado-Maior da Força.

Figura 1 - Antena satélite GIGASAT na Banda X

Figura 2 - Antena satélite AIRBUS na Banda C

O objetivo das duas redes é complementarem-se e garantir a redundância da rede SIC-Op. Adicionalmente, foi implementada uma rede *Welfare* nas zonas de lazer e alojamentos, cuja ligação de internet está assente num terminal *Starlink da SpaceX*, para além de possibilitar acesso a conteúdos multimédia. Para a comunicação com familiares e amigos em TN, para além da internet, os militares da Força dispõem de telefones instalados nos alojamentos que, interligados com a rede SIC-Op, permitem comunicar para Portugal 24h por dia.

As Operações e o Apoio de CSI

Em situações em que a FND não é projetada para missões para fora da capital Bangui, nos seus deslocamentos na cidade, as viaturas URO VAMTAC da Unidade de Manobra, usando o rádio PRC-525 e os rádios TETRA da MINUSCA, são seguidas pelo Centro de Operações Táticas (COT), através de aplicações de tracking – *Battlefield Management System* (BMS) e Gina (aplicação de *tracking* através do TETRA).

Se a missão atribuída for fora da zona de Bangui, então parte do ModCom segue projetado com a Força, garantindo o apoio de CSI no Posto de Comando Avançado, vulgarmente designado como *Temporary Operational Base* (TOB). Este apoio é conseguido através de um módulo do Sistema de Informação e Comunicações Tático (SIC-T), no caso, uma viatura Centro de Comunicações de Companhia (CCC). Nesta situação, todos os serviços na TOB são garantidos como na MOB. Na TOB, a ligação para TN é efetuada pelo terminal satélite *DataPath* CCT-200 (Figura 3). A ligação de internet é garantida através do terminal Starlink, com larguras de banda em torno dos 200 Mbps, garantindo todas as atividades de trabalho e planeamento da Força e fornecimento de internet de *Welfare* para os militares projetados. De realçar que a TOB e a MOB estão *online* simultaneamente e há sempre ligações garantidas, quer entre os dois Postos de Comando, quer com o TN.

Figura 3 - Terminal satélite DataPath CCT-200

No período dos 6 meses de missão, a 14ªFND/MINUSCA efetuou uma grande missão conjunta no exterior de Bangui. Numa primeira fase, consistiu na projeção aérea de um pelotão da Unidade de Manobra para a região de Zémio, a aproximadamente 1000 km da capital, juntamente com o proporcional de apoio de combate, nomeadamente um militar do ModCom. Numa segunda fase, efetuou-se a projeção terrestre com outro Pelotão da Unidade de Manobra e uma estrutura de Comando e Estado-Maior, assim como 3 militares do ModCom, com a finalidade de reforçar o pelotão já presente que foi projetado via aérea. Esta missão como um todo teve o objetivo primordial de reforçar a presença militar na região, garantindo para um ambiente mais seguro e estável. De salientar que esta operação como um todo, levou a que militares estivessem mais de 50 dias projetados fora do Campo Portugal.

Principais desafios

O TO da RCA é extremamente exigente ao nível do apoio de CSI. A tipologia de missão (combate) causa um grande desgaste no material, sobretudo no equipamento individual de comunicações dos militares. As rigorosas condições climatéricas (calor, vento e chuva forte) colocam em causa, recorrentemente, a operacionalidade dos equipamentos, bem como a estabilidade da rede. Mais ainda quando os equipamentos utilizados não estão preparados para fazer face a este tipo de condições climatéricas. O pó recorrente no ar, sobretudo nos deslocamentos (os itinerários são praticamente todos em terra batida), é mais um elemento propício para o aparecimento de avarias. Sendo um TO longínquo e com algumas limitações de material sobressalente/reserva, a inoperacionalidade de determinado equipamento não é de fácil substituição, devendo os militares, muitas vezes, terem a capacidade de reparar os equipamentos no próprio local. Em suma, o TO da RCA é um verdadeiro desafio a um normal apoio de CSI.

Módulo de Comunicações da 5FND/ROU

Tenente Tm Ana Catarino
Comandante do Módulo de Comunicações e Sistemas de Informação da 5ªFND/ROU

No âmbito das *Enhanced Vigilance Activities* da Organização do Tratado do Atlântico Norte, na Roménia, o Módulo de Comunicações e Sistemas de Informação integrado na 5ª Força Nacional Destacada Companhia de Atiradores da Roménia (5ª FND CAtMec/ROU) tem um papel determinante para garantir o exercício do Comando e Controlo (C2) ao Comandante da Força e a toda a sua estrutura hierárquica.

O módulo é composto por sete militares, um oficial, três sargentos e três praças, para fazer face ao cumprimento de todas as tarefas, tarefas essas realizadas em aquartelamento, em Caracal, bem como em projeção a fim da força participar em exercícios multinacionais com outras forças NATO. Nesta tipologia de missão, é essencial que os militares sejam polivalentes, tenham conhecimento técnico e experiência nas diversas áreas de comunicações. Como toda a Força Nacional Destacada (FND) a capacidade de *rear link*, isto é, comunicações entre o Teatro de Operações (TO) e o Território Nacional é essencial. Em aquartelamento, essa valência é assegurada por uma ligação satélite, através de uma antena satélite *DataPath* CCT 200 com uma largura de banda flexível consoante a disponibilidade da banda X atribuída à FND por parte da DIRCSI/EMGFA. Quando em projeção, juntamente com a *SHELTER*, viatura de comunicações – Centro de Comunicações de Companhia (CCC) esta capacidade é assegurada através do terminal satélite *Starlink da Spacex* juntamento com um MOCSITO fornecendo os serviços da RDE em projeção.

Figura 1 - Constituição do Módulo de Comunicações

O acesso à internet no aquartelamento quer para a rede de trabalho como para a moral e bem-estar (*Welfare*) foi desde o início (baseada no *Technical Agreement*), suportada pela rede interna do 1ª Batalhão de Instrução romeno, através da operadora DIGI, tendo como redundância o terminal satélite *Starlink* quando não usado em projeção. Ao contrário de outros TO, este apresenta uma variada infraestrutura de comunicações, fornecendo internet de qualidade à FND tanto em aquartelamento como na projeção.

Figura 2 - SHELTER, Centro de Comunicações (CCC)

As comunicações internas da FND CAtMec/ROU na Roménia são baseadas em meios rádios, PRC-525, PRR H4855 e telefone satélite IRIDIUM. Em exercícios multinacionais todos os meios rádios são essenciais para o C2 da Força, sendo o Rádio Tático 525 (PRC-525) equipado em todas as viaturas táticas. De forma a incrementar o C2 da Força em operação, o sistema BMS (*Battlefield Management System*) foi implementado nas viaturas táticas, tendo sido uma mais valia para o planeamento das operações e ainda para o comando e controlo de todos os movimentos. Uma vulnerabilidade apresentada em exercícios com outras forças NATO, é a carência de interoperabilidade de meios rádios operados em rede segura, sendo a mesma colmatada com a troca de operador entre forças, de forma a permitir a comunicação entre ambas.

A nível de comunicações seguras, a FND disponibiliza ainda de um gestor de *emails* de rede SECNET e NSWAN, sendo a mesma operada pelo Módulo Conjunto de Informações (MCI) e pelo Comandante da Força.

Figura 3 - Comunicações internas numa viatura PANDUR

Figura 4 - Comunicações com rádio PRC-525 versão MANPACK

O TO Roménia apesar de apresentar um nível de risco inferior em comparação com outros é de igual forma exigente, sendo um exemplo da cooperação entre Portugal e os Aliados no exercício de persuasão na frente Leste, sendo imprescindível que a Força tenha à sua disposição recursos e soluções tecnológicas atualizadas que auxiliem no C2 nas operações.

Domínio Invisível - A evolução da Guerra Eletrónica na Guerra da Ucrânia

Capitão Tm Miguel Gonçalves
Comandante da Companhia de Guerra Eletrónica

Introdução

O espectro eletromagnético desempenha um papel fulcral nos conflitos atuais, sendo um ativo crítico para as operações militares modernas. Através dele é possível efetuar comunicações, utilizar sistemas de navegação, controlar sistemas de armas, entre outras aplicações, tornando-o numa ferramenta essencial para exponenciar o potencial de combate de qualquer força. A crescente dependência tecnológica na arte de fazer a Guerra, eleva a importância de garantir a superioridade e supremacia do espectro eletromagnético, como forma de obter vantagem sobre o adversário. A materialização desta vantagem recai, em grande parte, na implementação e operacionalização de uma capacidade efetiva de Guerra Eletrónica (GE), estando atualmente esta capacidade a definir o campo de batalha de forma invisível, mas profundamente impactante.

Anualmente a 15 de abril a Federação Russa celebra o dia do "Especialista de Guerra Eletrónica". Neste dia, em 1904, decorria a Guerra Russo-Japonesa quando a Rússia utilizou pela primeira fez na história mundial a capacidade de Guerra Eletrónica em combate, na denominada Batalha de *Port Arthur*. Os navios nipónicos "Kasuga" e "Nissin" atacavam a base naval Russa de Port Arthur, situada no extremo sul da península de Liaodong, na China, quando os militares de comunicações que prestavam serviço no navio de guerra Russo "Pobeda" e na Estação Telegráfica de Costa aí existente, causaram com os seus equipamentos de comunicações interferências rádio que impediram o bom funcionamento da rede de comando e controlo da Marinha Japonesa nesta Operação. Esta ação impediu a realização de um bombardeamento eficaz por parte das tropas japonesas, materializado assim a primeira ativação de Contra Medidas Eletrónicas (CME) da história. Existe pois, pelo apresentado, um forte legado histórico da importância que a Rússia coloca na sua capacidade real de GE [1][2].

Após 2014, quando a Federação Russa anexou a Crimeia, as capacidades tecnológicas em GE evoluíram mais que nunca, como uma ferramenta de domínio estratégico, transformando o modo como as nações se preparam e enfrentam os conflitos. O conflito na Síria, iniciado em setembro de 2015, deu à Rússia o palco perfeito para testar em combate uma ampla gama de sistemas de GE, incluindo protótipos. A invasão da Ucrânia pela Rússia em fevereiro de 2022, apoiada pela experiência adquirida desde 2014, veio exponenciar a inovação tecnológica com especial foco na capacidade de Guerra Eletrónica.

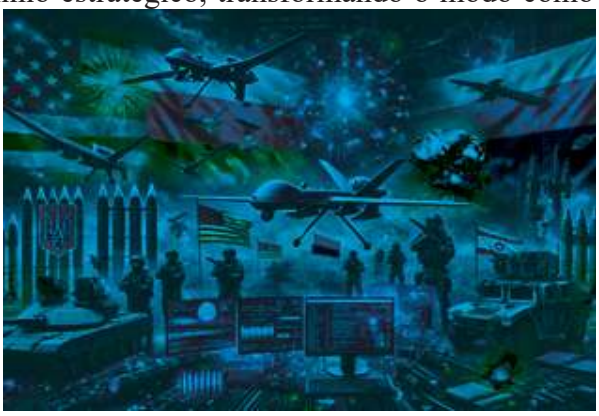


Figura 1- Uma guerra multidomínio com o espectro eletromagnético a ser a principal ferramenta de trabalho.
Fonte:https://tribunadelabahia.com.mx/inteligencia-artificial-predice-guerra/

Sobre estas temáticas, a informação em fontes abertas é escaca e pouco detalhada, no entanto, pretende-se com este artigo examinar a evolução da Guerra Eletrónica desde 2014, abordando as capacidades de GE Russas e Ucranianas na invasão da Crimeia em 2014, a preparação da Rússia para a invasão em 2022, a sua execução e o papel revolucionários dos Drones neste conflito.

Guerra da Ucrânia: o *Silicon Valley* da Guerra Eletrónica de última geração

A invasão da Crimeia

Em fevereiro de 2014, após a destituição do Presidente Ucraniano Viktor Yanukovych, a Rússia iniciou uma série de ações para assegurar a sua influência sobre a península da Crimeia, região de elevada importância estratégica e com uma população maioritariamente pró-Russa. Em março de 2014, um referendo realizado na Crimeia, dava uma maioria categórica a favor da reunificação com a Rússia (95,5%). Embora o referendo tenha sido amplamente contestado pela comunidade internacional, a Rússia formalizou a anexação da Crimeia pouco depois, materializando a "mais suave" invasão da era moderna, conforme escreveu o jornalista da BBC, John Simpson [3].

A invasão da Crimeia em 2014, apresentou uma capacidade de GE Russa substancialmente superior à da Ucrânia, tendo esta sido preparada entre os anos de 2010 e 2013, onde a Rússia desenvolveu 18 sistemas integrados de GE, dos quais apenas 14 se sabe o nome e que se descriminam em seguida: Borisoglebsk-2, Alurgit, Infauna, Krasukha-2O, Krasukha-S4, Moskva-1, Parodist, Lorandit-M, Leer-2, Leer-3, Lesochek, Less, Magnii-REB e o Pole-21 [4].

Durante a invasão da Crimeia em 2014, a capacidade de GE foi fundamental para o sucesso das operações, sendo que a Rússia demonstrou larga superioridade tecnológica face ao seu oponente. Nesta primeira invasão, foi enviada para a Crimeira, pelo menos uma Companhia de Guerra Eletrónica em suporte às forças terrestres, equipada com, pelo menos [2]:

• **03 *Leer-3 Systems*:** Sistema de GE não tripulado, constituído por 03 Orlan-10 UAVs e uma viatura posto de comando, com o objetivo de suprimir estações de base de comunicações móveis e substituí-las por estações de base virtuais falsas. Esta capacidade permitia executar operações de deceção através do envio de mensagens de texto falsas para as tropas ucranianas, afim de as desmoralizar;

Figura 2 - Sistema LEER-03.
Fonte: https://armyrecognition.com/news/army-news/2022/russian-troops-using-leer-3-able-to-jam-ukrainian-army-mobile-phone-signals-within-30-km

• **01 *Borisoglebsk-2B*:** com capacidade de monitorização do espectro, radiolocalização e empastelamento nas bandas HF/VHF/UHF, era capaz de obter sinais em frequência fixa e com salto em frequência. Foi maioritariamente utilizado para a disrupção das comunicações VHF táticas Ucranianas;

• **02 *R-330Zh Zhitel*:** com capacidade de monitorização do espectro (100MHz-2GHz), radiolocalização e empastelamento de comunicações satélite, links de controlo de UAVs e sistemas de navegação;

• **02 *RP-377LA Lorandit*:** com capacidade de monitorização do espetro e de empastelamento de comunicações HF/VHF/UHF. Opera entre os 20MHz e os 2GHz. Permite empastelamento de comunicações com um máximo de 100W de potência;

Figura 3-RP-377LA Lorandit
Fonte: https://armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/ukrainian-forces-destroy-rp-377la-lorandit-crucial-player-in-russian-army-s-electronic-warfare

• **02 R-934B V/UHF:** Sistema de empastelamento automático para comunicações em VHF, Tem a capacidade de detetar, analisar, radiolocalizar e empastelar links rádio em VHF com uma frequência de salto de até 1000 saltos por segundo. Frequentemente usado para anular comunicações terra-ar com aeronaves ucranianas;

Figura 4 - Sistema R-934B V/UHF
Fonte:https://roe.ru/eng/catalog/land-forces/reconnaissance-and-ew/army-ew/r-934b/

À data, sabe-se que equipavam ainda a capacidade de GE Russa, entre outro, os seguintes equipamentos (que se destacam pela sua importância estratégica):

• **Murmansk-BN:** Sistema transportável de empastelamento estático desenhado para atacar as redes de HF Ucranianas a longas distâncias;

• **Krasukha-4:** Sistema para deteção de longo alcance (200-250 Km) de sinais radar provenientes de aeronaves. Permite o empastelamento de sinais de radar. Especialmente focado em radares de aeronaves, misseis guiados por radar e UAVs, opera na entre os 8GHz e os 18GHz.

Figura 5-Sistema Murmansk-BN
Fonte: https://www.armyrecognition.com/military-products/army/electronic-warfare/murmansk-bn-electronic-warfare-communications-jamming-systemdata?highlight=WyJydXNzaWEiXQ%3D%3D

Em contrapartida, a Ucrânia enfrentava desafios significativos. Durante os anos anteriores, a Ucrânia não priorizou suficientemente o desenvolvimento de capacidades de guerra eletrónica e muitas das unidades ucranianas tinham sistemas antigos ou pouco equipados. Os seus sistemas de GE baseavam-se em tecnologias da Era Soviética, incapazes de neutralizar as operações russas. A vulnerabilidade ucraniana destacou a necessidade urgente de investimentos e apoio internacional.

Figura 6- Sistema Krasukha
Fonte: https://armyrecognition.com/focus-analysis-conflicts/army/defence-security-industry-technology/analysis-how-russia-s-krasukha-electronic-warfare-system-disrupts-uavs-and-radars-in-ukraine

A Ucrânia utilizava, à data, sistemas como: Kolchuga para deteção de radar, que pode fornecer informações cruciais sobre as movimentações do inimigo; Mandat-B1E para realizar interferências nas comunicações, projetado para bloquear sinais de comunicações táticas e interromper as redes de comunicação do inimigo. [2][3].

Figura 8 – Sistema Kolchuga
Fonte: https://armyrecognition.com/news/army-news/army-news-2022/ukrainian-army-upgrading-kolchuga

Figura 7-Mandat-B1E
Fonte:http://uoe.com.ua/products/en/?id=0&pid=catalogue&language=eng&catalogue_id=549&type=content

A invasão da Ucrânia em 2022:

A preparação:

O programa de desenvolvimento da capacidade de GE Russa decorreu entre 2011 e 2020 e revitalizou com grande relevância o vetor material, mas não só. Neste período decorreu também uma reorganização na Ordem de Batalha dos ativos de GE Russos. Foram criadas Brigadas de GE para garantir apoio ao nível operacional e cada unidade de manobra de escalão Divisão ou Brigada tinha a sua Companhia de GE independente. Para garantir o apoio mútuo de GE e fazer o *link* entre o nível operacional das brigadas de GE e o nível tático das companhias, foram criados Batalhões de GE que eram alocados às *Russia's Combined Arms Armies* (CAAs), cada uma responsável por um distrito militar definido [5].

Além da massificação na produção dos equipamentos existentes, a Rússia lança um novo equipamento, o *Divnomorye-U* capaz de substituir três dos sistemas Russos em produção: o Krasukha 2 e 4 e o Moskva-1. Este novo equipamento permite a criação de uma bolha de interferência de centenas de quilómetros para proteção de sinais radar hostis. É de tal forma capaz que foi comprovada a sua eficácia contra alguns sistemas Americanos, tais como o E-8 JSTAR, E-3 AWACS e E-2 HAWKEYE, sendo também eficaz contra UAVs. [5]

Enquanto a Rússia se massificava na capacidade de GE, a Ucrânia focou-se em desenvolver uma resiliência eletrónica com apoio externo. Equipamentos fornecidos pela NATO e sistemas de comunicação seguros minimizaram a sua vulnerabilidade frente à superioridade Russa.

A Ucrânia, com apoio das nações ocidentais, iniciou uma transformação significativa. Em 2016 entrou ao serviço da GE ucraniana o "Plastun-3000RP", um *man-portable direction finder* e em 2018, uma versão deste equipamento numa viatura tática média, designado por "Khortytsia-M". A aquisição de sistemas como o "Bukovel-AD", para neutralizar drones e bloquear sinais de GPS fortaleceu a sua capacidade defensiva [6].

Figura 9 - Bukovel
Fonte : https://armyrecognition.com/news/army-news/army-news-2019/morocco-buys-ukrainian-bukovel-ad-drone-detection-system

Fevereiro de 2022- A invasão:

Fevereiro de 2022 foi palco de uma das maiores projeções da história de ativos de GE, por parte da força Russa. Estudos apontam para que tenham sido projetadas as 6 Brigadas Terrestres de GE que a Rússia dispõe, apoiadas por 12 Batalhões de GE e 28 Companhias de GE [2].

Embora impressione pela quantidade, o efeito criado por estas unidades fora um pouco menos impressionante. "A Rússia não preparou muito bem as suas forças de EW", comentou Iaroslav Kalinin, diretor executivo da Infozahyst, uma empresa ucraniana atualmente dedicada à produção de equipamentos de GE [2].

A capacidade Russa contra sinais *Positioning, Navigation and Timing* (PNT) e sinais de comunicações móveis não foi além da capacidade de radiolocalização. A capacidade de empastelamento de radar Russa não foi eficaz contra os radares de vigilância aérea ucranianos. Por estes motivos, no inicio da ofensiva Russa o Sistema Integrado de Defesa Aérea Ucraniano continuou operacional. As forças de GE Russas tentaram também disromper o acesso Ucraniano às redes *Starlink* e *Viasat* utilizando ciberataques, algo que não surtiu efeito de longa duração. À data da invasão as forças Russas não dispunham, alegadamente, de sistemas *Counter - Unmanned Aerial System* (C-UAS), capacidade que vieram a desenvolver mais tarde de forma significativa. As forças Russas de GE tiveram substancial sucesso contra rede V/UHF não encriptadas Ucranianas, no entanto o mesmo efeito não se sentiu em sistemas seguros, como por exemplo contra os Rádios L3Harris AN/PRC-152A Falcon III, fornecidos pelos Estado Unidos em 2014, que utilizam a forma de onda *SINCGARS*, que se verificou ser resistente ao empastelamento Russo [2].

Figura 10 - L3Harris AN/PRC-152A Falcon III
Fonte:[6]

A tática de GE Ucraniana na linha da frente:

Na linha da frente a Ucrânia tem utilizado com sucesso o "Plastun-RP3000", de fabrico Ucraniano, tendo a capacidade de monitorizar o espectro e radiolocalizar sinais entre os 25 MHz e os 3 GHz, num raio de aproximadamente 15 Km. É complementado à retaguarda pelo "Khortytsia-M" que opera na mesma banda, mas é capaz de detetar sinais a 45 Km de distância. A definição tática para a utilização destes dois equipamentos mostra-se na figura seguinte: [6]

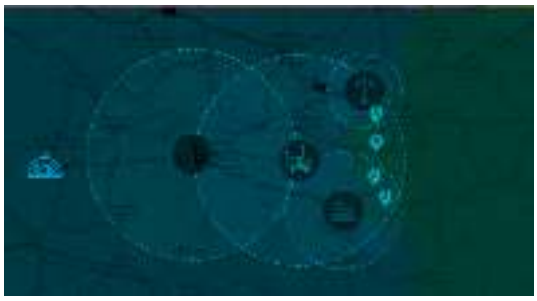


Figura 11 - Disposição tática no terreno dos equipamentos Ucranianos de monitorização de Espectro.
Fonte: [6]

Figura 12- Sistema Khortytsia-M
Fonte: [6]

Figura 13 – Sistema Plastun-RP3000
Fonte:[6]

Ambos produzidos pela Ucrânia, destaca-se o custo reduzido do *Plastum – RP3000*, o que permitiu à Ucrânia dispor de múltiplos equipamentos em cada Brigada, aumentando assim a malha de sensores no terreno. A radiolocalização dos 2 sistemas a trabalhar em conjunto constituiu-se, para os Comandantes aos vários níveis, uma ferramenta essencial para o aviso oportuno da ameaça e para o seguimento da atividade hostil [6].

Ouvidos Surdos e o jogo do Gato e do Rato

Equipamentos de comunicações obsoletos e pouca proficiência técnica dos soldados Russos, foram alguns dos grandes problemas enfrentados durante a ofensiva Russa em 2022. No início da invasão os baixos escalões das forças Russas usavam o rádio de fabrico Russo, An R-168 -0,5UM, produzido pela Al- Akveduk, que entrou ao serviço em 2020. A sua utilização enfrentou constantes falhas de comunicação devido à falta de fiabilidade do equipamento, tendo sido apontado como uma das principais causas da falta de precisão das unidades de Artilharia.

Figura 14 - Rádio Russo - An R-168 -0,5UM
Fonte:[6]

Agregado ao fator anterior, a falta de mecanismos de *Communications security* (COMSEC) deste equipamento deixava o trabalho facilitado para as forças de GE Ucranianas. A Rússia viu-se forçada a veicular as suas comunicações táticas em rádios civis, essencialmente em rádios *Digital Mobile Radio* (DMR) da empresa chinesa Hytera, que eram também facilmente intercetados pelos sistemas "Plastum – RP3000" Ucranianos[6].

No inicio de 2023, a Rússia viu-se obrigada a equipar as suas Unidades táticas com o seu Rádio Azart-2 com 3 versões: 187P1 Azart-P *short- range*: versão handheld (4 km de alcance) e que opera entre os 27 e os 520 MHz; R-187N Azart-N medium-range (12 km de alcance) e o R-187BV 'Azart-BV longer range (40 km de alcance), estes dois últimos montados em versão veicular. Sabe-se, no entanto, que apenas a versão *Handheld* foi colocada ao serviço, continuando os mais modernos Carros de Combate Russos, os T-80BVM e os T-90M, a utilizar os velhos rádios da família Al-Akveduk. Embora fosse um rádio de última geração, demonstrou falta de robustez, com uma complexidade de utilização elevada, fatores que aliados à falta de conhecimento técnico e treino dos soldados Russos levou a que algumas unidades retrocedessem e voltassem a utilizar o sistema de comunicações da Al-Akveduk e DMR civis, ficando altamente expostas às ações de GE Ucranianas [6].

Figura 15 – Rádio Russo 187P1 Azart-P
Fonte:[6]

Por seu lado a Ucrânia, por forma a reduzir a pegada eletromagnética, utiliza um rádio de fabrico Ucraniano, denominado Himera-G1 capaz de garantir comunicações seguras, com uma característica interessante: mantendo o alcance necessário para ser efetivo, emite 25 vezes menos potência que os rádios russos referidos anteriormente, o que o torna praticamente invisível aos olhos da GE Russa [2].

Figura 16- Rádio Himera-G1
Fonte: https://mil.in.ua/en/news/a-new-ukrainian-himera-g1-pro-radio-was-presented/

Empastelar o Recetor - A ameaça aérea:

Nem só de Guerra Eletrónica Terrestre vive a Guerra e, a Ucrânia tem vivido intensamente esta realidade com a realização de operações multi-domínio Russas. A evolução desde o início do conflito da capacidade de GE Russa, integrada nos diferentes domínios operacionais foi sem dúvida relevante, sendo um exemplo dessa modernização, a capacidade de empastelamento por vetor aéreo. A Rússia utiliza atualmente o helicóptero Mi-8MTPR-1 para transportar o sistema de empastelamento de sinais radar "Rychag-AV" e atacar os sistemas de defesa aéreos Ucranianos. Este sistema opera entre os 5.1GHz e os 11GHz e gera 500 000 pulsos por segundo, impossibilitando o radar recetor de efetuar o processamento dos pulsos, causando assim um ataque similar a um *Denial of Service attack* (DDoS) ao Sistemas de *Electronics Intelligence* (ELINT) dos sistemas de defesa aéreos Ucranianos, impedindo-os de detetar as aeronaves Russas. [6]

Figura 17 - Ilustração do Mi-8MTPR-1 a empastelar os sistemas de defesa aéreos ucranianos

Outros assets Russos relevantes:

As tropas russas têm utilizado para a deteção de comunicações táticas, radiolocalização e empastelamento de links de comunicações Ucranianas o sistema TORN, que tem especial foco nas bandas VHF/UHF e comunicações móveis (1.5MHz a 3.0 GHz) [7].

Figura 18 - R-934B Sinitsa
Fonte: https://mil.in.ua/en/news/ukrainian-military-destroys-russian-r-934b-sinitsa-electronic-warfare-station/

Não menos importante, o sistema RB-636 SVET-KU é capaz de empastelar sinais rádio e radar (25 MHz aos18 GHz) e os empasteladores R-934B Sinitsa e R-330Zh Zhitels são responsáveis pelos sinais de satélite.

Também o Krasukha-4 continua a operar, materializando o bloqueio de sinais radar do adversário, interromper as ligações a satélites de órbita baixa terrestre e perturbar os radares de *Airborne Early warning and control* (AEW&C) [7].

É interessante perceber que os equipamentos russos de empastamento de sinais satélite são atualmente bastante eficazes, sendo conhecido que foram capazes de degradar o *M-Code Signals* da constelação *GPS* dos *USA*, com graves consequências nas atividades comerciais, pois também é negado o acesso ao sistema de navegação de entidades civis que estejam na área de cobertura do empastelador. Na figura seguinte podemos observar um mapa, referente ao dia 27 de janeiro de 2024, com a georreferenciação dos locais alvo de empastelamento de *GPS* por parte da Rússia [8].

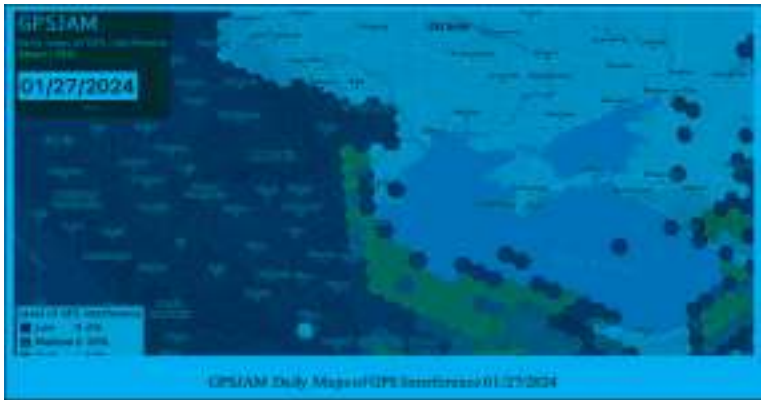


Figura 19 - Mapa com o registo de Interferências GPS no dia 01JAN24.
Fonte:[8]

Drones: A nova ameaça

Os drones são, de ambos os lados, a ameaça mais presente atualmente no campo de batalha. Para combater essas ameaças, ambas as fações adotaram tecnologias como:

• Sistemas de Jamming: Interferem nos sinais de controlo e GPS dos drones;

• Radares de Alta Frequência: Detetam drones a operar em baixa altitude;

• Armas de Energia Dirigida: Desenvolvidas para destruir drones directamente com lasers ou micro-ondas.

Uma lição aprendida pelas forças ucranianas após quase 3 anos de Guerra prende-se com a necessidade de garantir proteção eletrónica contra UAVs a todas as unidades táticas de baixo escalão, havendo a necessidade de distribuir equipamentos de GE a todas as forças de manobra. Aprenderam ainda que, os sistemas de GE projetados aos níveis táticos têm de ser fáceis de substituir, têm que ser produzidos em larga escala e ser capazes de efetuar várias missões [2].

Figura 20 –Jammer ucraniano anti-drone portátil.
Fonte: https://euromaidanpress.com/2024/05/17/the-ew-back-pack-revolution-how-ukrainian-portable-tech-jams-russian-drones/

Nesta temática a Rússia enfrentou um sério problema, comumente designado por fratricídio eletromagnético, aquando das suas tentativas de empastelar UAVs Ucranianos. Estes defrontaram problemas de incompatibilidade entre os seus empasteladores e alguns dos seus equipamentos de comunicações utilizados em unidades de baixo escalão para comunicações *intra-team* que, tipicamente, utilizam a banda do UHF para comunicar. As unidades de GE Russas foram obrigadas a reduzir a sua capacidade de empastelamento, o que permitiu à Ucrânia explorar o envio de UAVs com cargas cinéticas, causado consequências devastadoras [2].

Se por um lado a quantidade de UAVs no campo de batalha aumentou exponencialmente, aumentou também a resposta *anti-drone*, com o surgimento de armas de energia dirigida. São exemplos utilizados pela Russia a Harpoon-3 e Silok systems[9]:

Figura 21 - Harpoon-3
Fonte:[9]

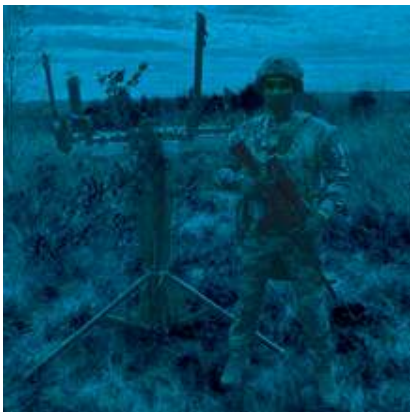


Figura 22 - Silok Systems
Fonte:[10]

Neste campo a Ucrânia também tem dado passos largos na procura da melhor solução C-UAS. Alguns exemplos de equipamentos atualmente em produção na Ucrânia são: o EDM4S (*Electronic Drone Mitigation System*) e o SKY CTRL *anti-drone system*, dois sistemas de energia dirigida anti-drone, um na forma de arma e outro montado num tripé. Adaptado à evolução tecnológica e ao surgimento em massa de drones *first person view* (FPV) Russos, a empresa ucraniana Kvertus fornece atualmente para o campo de batalha um dispositivo para colocar às costas de cada militar, criando uma bolha eletromagnética em seu redor impedido que o drone inimigo se aproxime (figura 25) [11].

Figura 23 - EDM4S
Fonte: https://mezha.media/en/2022/06/13/110-lithuanian-edm4s-anti-drone-rifles-for-the-armed-forces/

Figura 24 - SKY CTRL
Fonte: https://mil.in.ua/en/news/the-ukrainian-military-received-the-sky-ctrl-anti-drone-system/#google_vignette

Figura 25 – KVERTUS F2M5
Fonte:https://kvertus.ua/en/product/kvertus-ad-counter-fpv-backp

A última inovação da Ucrânia foi desvendada em dezembro de 2024, onde foi anunciada uma Laser Gun, denominada de Tryzub que será capaz de destruir uma aeronave a uma altitude máxima de aproximadamente 2 Km. Uma solução comparável com a *LaWS* dos *USA* e com a *DragonFire* usada pelo Reino Unido[12].

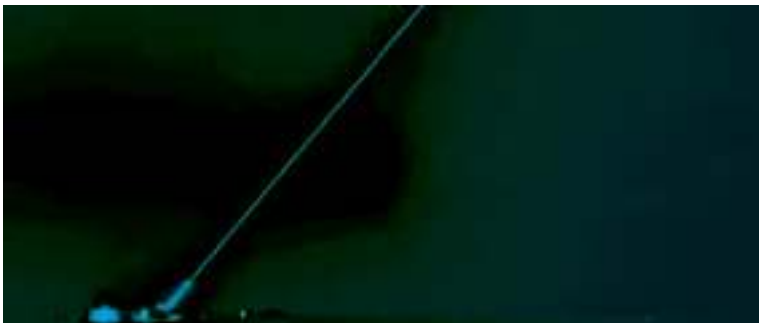


Figura 26 – Arma de Energia Dirigida Ucrâniana "Tryzub" em fase final de testes.
Fonte:[12]

Estas soluções redefiniram as prioridades da GE, ampliando a sua relevância no campo de batalha. Suspeita-se que atualmente a Rússia tenha um sistema de GE a cada 2 Km de frente de combate e que aproximadamente 90% dos assets de GE empenhados no nível tático estejam focados na capacidade C-UAS, mostrando claramente a importância desta capacidade no campo de batalha atual [2].

Os especialistas Ucranianos foram obrigados a desenvolver táticas para evitar o cerco apertado da GE Russa, estando por exemplo a utilizar frequências de controlo de UAVs Russas para empenhar os seus UAVs, garantindo desta forma que o empastelamento Russo, a ser feito também afeta os seus próprios assets. Uma outra técnica utilizada pelas forças ucranianas reside na capacidade de colocar Inteligência Artificial a detetar uma ação do empastelamento e a conduzir de forma automática uma mudança na frequência de controlo do UAV para fora do alcance, em frequência, do empastelador Russo. Atualmente ambas as partes estão a apostar em equipamentos de baixo custo, conjugado com uma grande capacidade de substituição. [2]

Conclusões

A guerra moderna tornou-se um cenário onde o espectro eletromagnético define, em grande medida, o sucesso ou o fracasso das operações militares. Desde os primeiros esforços da Rússia na Guerra Russo-Japonesa até os dias de hoje, a evolução da Guerra Eletrónica (GE) reflete a crescente importância de dominar este domínio invisível, mas decisivo.

No conflito em curso na Ucrânia, a aplicação intensiva de capacidades de GE reafirma o compromisso Russo em explorar esta dimensão como uma ferramenta estratégica para obter superioridade operacional. A interferência nas comunicações, a neutralização de drones e a sabotagem de sistemas de navegação são apenas alguns exemplos de como a guerra eletrónica tem moldado o campo de batalha. Este cenário sublinha que, para além das forças convencionais, a supremacia tecnológica e a capacidade de operar eficazmente no espectro eletromagnético são agora fatores determinantes na definição do poder militar.

Por outro lado, a experiência ucraniana tem demonstrado que a adaptabilidade e a resiliência tecnológica também são cruciais. Dessa experiência saem algumas lições aprendidas [6]:

- Sistemas mais pequenos e mais baratos são melhores;
- Os sistemas de GE têm que estar distribuídos pela linha da frente, garantindo ao comandante a flexibilidade de reação e decisão;
- *Links* de comunicações inseguros são altamente vulneráveis;
- Colocar o operador de GE num local diferente do equipamento de GE, previne perdas humanas, no caso dos equipamentos serem atacados, o que é recorrente;

O uso criativo de soluções tecnológicas por parte da Ucrânia, frequentemente em resposta às capacidades Russas, exemplifica a crescente complexidade dos conflitos modernos. Isso reforça que o futuro da guerra será cada vez mais dominado por batalhas invisíveis, onde a guerra eletrónica e o controlo do espectro eletromagnético não serão apenas auxiliares, mas elementos centrais da estratégia militar.

Assim, é imperativo que as nações reconheçam e invistam neste domínio para assegurar a sua segurança e soberania. A história da Guerra Eletrónica, desde a Batalha de *Port Arthur* até os conflitos contemporâneos, ilustra que a superioridade no espectro eletromagnético não é apenas uma vantagem tática, mas um requisito estratégico para prevalecer nos cenários de guerra do futuro.

Figura 27 – Militares da CompGE no execício Viriato

Bibliografia:

[1] TOPWAR. (2021). April 15 - Day of the electronic warfare specialist of the Armed Forces of Russia. Disponível em: https://en.topwar.ru/181991-15-aprelja-den-specialista-po-radiojelektronnoj-borbe-vooruzhennyh-sil-rossii.html;

[2] WITHINGTON, Thomas. Electronic Warfare & the Tactical Land Battle in Ukraine. HERTZ&MINDS, 1 de novembro de 2024;

[3] BBC. Guerra na Ucrânia: o que é a 'linha de frente' e como ela mudou nos últimos dias. BBC News, 28 de março de 2022. Disponível em: https://www.bbc.com/portuguese/internacional-60570951;

[4] JED ONLINE. From the JED Archives: Tuning In, Turning On: Russia Brings Radio-Electronic Combat to the Fore. JED Online, 16 de fevereiro de 2023. Disponível em: https://www.jedonline.com/2023/02/16/from-the-jed-archives-tuning-in-turning-on-russia-brings-radio-electronic-combat-to-the-fore-2/;

[5] JAMESTOWN FOUNDATION. Russia's Military Boosts Electromagnetic Spectrum Capability. Jamestown, 9 de março de 2023. Disponível em: https://jamestown.org/program/russias-military-boosts-electromagnetic-spectrum-capability/;

[6] CAZALET, Mark. Silent Struggle: Accounts from the Frontlines of Ukraine's Electronic War. European Security & Defence, setembro de 2023;

[7] SOUSA, P. M. (2023). A Guerra da Ucrânia: O Sucesso da Artilharia e da Guerra Eletrónica. Revista Militar, 2653/2654. Disponível em: https://www.revistamilitar.pt/artigo/1700.

[8] CHIRIAC, O. R., & Withington, T. (2024). Russian Electronic Warfare: From History to Modern Battlefield. Irregular Warfare Initiative. Disponível em: https://irregularwarfare.org/articles/russian-electronic-warfare-from-history-to-modern-battlefield/.

[9] KADAM, T. (2022). Hitting With Harpoons! Russia Confirms Using Harpoon Systems To Shoot Down Ukrainian Suicide Drones. EurAsian Times. Disponível em: https://www.eurasiantimes.com/russia-use-harpoons-to-shoot-down-hostile-ukrainian-uavs-military/.

[10] AXE, D. (2024). Russia Deploys Silok Jammers To Ground Ukraine's Drones. Ukraine Hunts Down The Siloks With—You Guessed It—Drones. Forbes. Disponível em: https://www.forbes.com/sites/davidaxe/2024/01/21/russia-deploys-silok-jammers-to-ground-ukraines-drones-ukraine-hunts-down-the-siloks-with-you-guessed-it-drones/.

[11] MARTYNIUK, Y., & Ekonomichna Pravda. (2024). The EW Backpack Revolution: How Ukrainian Portable Tech Jams Russian Drones. Euromaidan Press. Disponível em: https://euromaidanpress.com/2024/05/17/the-ew-backpack-revolution-how-ukrainian-portable-tech-jams-russian-drones/.

[12] SUKHAREVSKYI, V. (2024). Testing begins of Ukraine's homegrown Tryzub laser weapon. Ukrainian World Congress. Disponível em: https://www.ukrainianworldcongress.org/testing-begins-of-ukraines-homegrown-tryzub-laser-weapon/.

Aprontamento e Projeção do PelCC 1FND/SVK – Desafios e Oportunidades para o SIC-T

Tenente Tm Ricardo Oliveira
Comandante da CTm/BrigMec

Resumo – O Exército recebeu a missão de aprontar e projetar um Pelotão de Carros de Combate, integrando uma Unidade de Escalão Batalhão Espanhola no *NATO Multinational Battlegroup*, na Eslováquia, por um período até seis meses. Esta Força foi projetada para o Teatro de Operações (TO) em julho de 2024.

O Pelotão de Carros de Combate está equipado com cinco Carros de Combate Leopard 2A6, guarnecidos por 24 militares, aos quais se somam três militares em funções de Estado-Maior, nos Quartéis-Generais da Unidade Escalão Brigada e do *Battlegroup*, num efetivo total de 27 militares.

O início do Aprontamento desta Força foi formalizado no dia 26 de janeiro, tendo a Companhia de Transmissões acompanhado em matéria de Comunicações e Sistemas de Informação (CSI).

Na sua Estrutura Orgânica, a Força conta com um Módulo de Transmissões, composto por um Sargento e uma Praça.

Durante os seis meses de aprontamento, nas atividades de Treino Orientado para a Missão e Exercícios em que Força participou, foram identificados alguns desafios do ponto de vista de comunicações. A macroestrutura CSI a instalar em TO (onde se incluem as comunicações estratégicas), a configuração e gestão de uma rede rádio VHF *full-IP*, a interoperabilidade com o Escalão Superior Multinacional e a configuração e gestão do *Battlefield Management System* foram alguns dos desafios identificados nesta fase.

Neste artigo pretende-se elaborar sobre estes tópicos, apresentando as soluções encontradas e realçando de que forma é que as mesmas se poderão configurar como oportunidades de evolução e melhoria para o Sistema de Informações e Comunicações – Tático (SIC-T).

Palavras-Chave: Comunicações e Sistemas de Informação

Introdução

A projeção de um Pelotão de Carros de Combate (PelCC) do Exército Português para a Eslováquia em junho de 2024 marca um importante capítulo na cooperação militar entre os dois países e na participação de Portugal nas operações de defesa coletiva da NATO. Este Pelotão integrou uma Unidade de Escalão Batalhão Espanhola no *NATO Multinational Battlegroup*. A Brigada Mecanizada constituiu-se como Unidade Mobilizadora desta Força Nacional Destacada, tendo o aprontamento da Força decorrido ao longo de seis meses no Campo Militar de Santa Margarida, campo de manobras por excelência em Portugal.

A projeção desta Força teve como objetivos reforçar a defesa coletiva da Aliança, contribuir para a segurança do flanco leste da mesma, assegurando uma presença militar dissuasora, promover a interoperabilidade através do treino e operação em conjunto com as forças eslovacas e de outros países da NATO, melhorando a coordenação e a eficácia das ações conjuntas e reforçando o compromisso de Portugal com os seus aliados e com os princípios da NATO, bem como com a paz e a estabilidade europeias.

A Força Nacional Destacada, equipada com cinco Carros de Combate Leopard 2A6, guarnecidos por 24 militares, contempla na sua Estrutura Orgânica um Módulo de Transmissões, constituído por um Sargento e por uma Praça, oriundos da Companhia de Transmissões da Brigada Mecanizada.

No decorrer da fase de Treino Orientado para a Missão foram identificados alguns desafios para o Sistema de Informações e Comunicações – Tático, decorrentes, não só da tipologia de força a projetar, mas também do escalão da mesma. Este artigo pretende elencar os desafios encontrados, apresentando as soluções encontradas e realçando de que forma é que as mesmas se poderão configurar como oportunidades de evolução e melhoria para o Sistema de Informações e Comunicações – Tático (SIC-T).

Figura 1 - Manutenção de Equipamentos Rádio

Conceito de Apoio de Comunicações

A 1ª Força Nacional Destacada para o Teatro de Operações da Eslováquia é uma Unidade Escalão Pelotão equipada com Carros de Combate Leopard 2A6.

A estrutura de comunicações do Pelotão de Carros de Combate assenta primariamente em duas redes rádio VHF: Rede de Comando e Operações e Rede Administrativo-Logística, ambas em SECOM-V.

Adicionalmente, cada Carro de Combate está equipado com um Terminal de Dados Portátil Robustecido que serve de plataforma para o *Battlefield Management System* (BMS), ferramenta que permite ao Comandante do PelCC a visualização da *Common Operational Picture* (COP) na condução de operações.

A interligação com o Escalão Superior Multinacional obtém-se através da utilização de rádio compatível com chaves NATO, instalado no Carro de Combate Leopard 2A6.

Figura 2 - Atividade de Treino Operacional na Eslováquia

Desafios

No decorrer da fase do Treino Orientado para a Missão, durante o aprontamento do PelCC, foram identificados alguns desafios no que diz respeito às Comunicações e Sistemas de Informação, sendo descritos e detalhados de seguida.

Numa fase inicial, no decorrer do planeamento da estrutura das redes rádio e posterior configuração das mesmas, definiu-se como pré-requisito que estas fossem *full-IP*, de forma a obter uma integração total entre o Sistema de Informações e Comunicações Tático e Operacional. Em Território Nacional, esta integração fez-se por meio de uma estação rádio 525 que fez a interligação entre a rede de Comando e Operações do PelCC e os serviços disponibilizados no SIC-Op.

Figura 3 - BMS num CC Leopard 2A6

Na fase de preparação para a Inspeção Operacional do PelCC, recorreu-se a um servidor configurado com *Networked Interoperable Real-time Information Services* (NIRIS) e a um servidor *Interim Geo-Spatial Intelligence Tool* (iGeoSIT) para incluir o PelCC na COP da Brigada Mecanizada. Esta integração do sistema BMS do PelCC foi possível graças à configuração da rede rádio VHF em *full-IP* e da interligação da mesma com o SIC-T.

Um desafio transversal à fase aprontamento e projeção do PelCC no âmbito das Comunicações e Sistemas de Informação prendeu-se com a definição da estrutura de redes de computadores a instalar em TO. Sendo este um escalão atípico relativamente ao empenhamento de forças em compromissos internacionais, verificou-se alguma dificuldade em adequar a doutrina e a experiência existentes às necessidades de meios a projetar, tendo em última instância sido adotada uma solução que favoreceu a simplicidade.

Também a interoperabilidade necessária à condução de operações num ambiente multinacional se revelou como um desafio, uma vez que os equipamentos da família do PRC525 apresentam alguns constrangimentos de ordem técnica neste aspeto, tendo-se recorrido, para o efeito, à integração de equipamentos rádio no sistema de comunicações do Leopard que cumprem as especificações da NATO para a interoperabilidade.

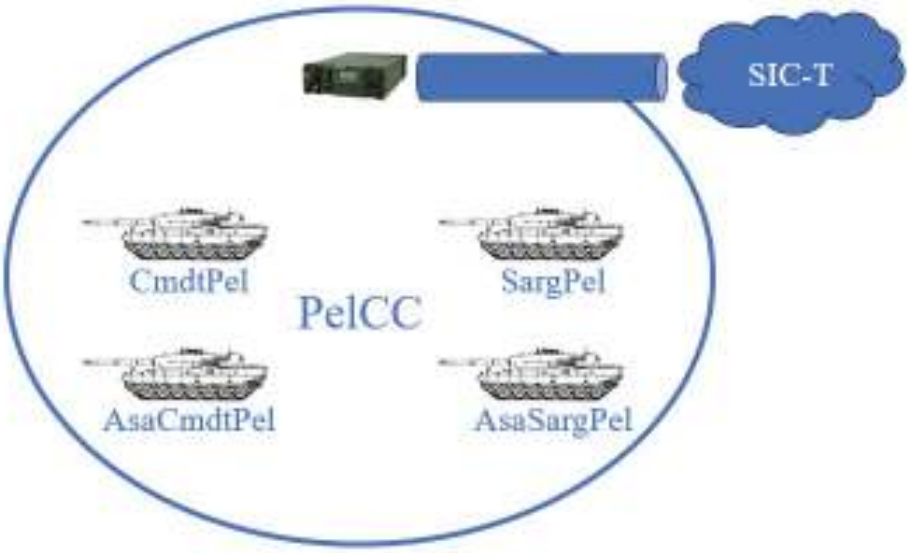


Figura 4 - Esquema de rede VHF e integração com SIC-T

Conclusões

O aprontamento e projeção de um Pelotão de Carros de Combate para a Eslováquia teve, naturalmente, alguns desafios no que às Comunicações e Sistemas de Informação diz respeito, sendo esta uma área crítica para a garantia do Comando e Controlo do Comandante de Pelotão.

No presente artigo pretendeu-se enumerar os desafios de ordem técnica encontrados e de que forma estes podem contribuir para uma abordagem e adaptação dos princípios de aplicação do Sistema de Informações e Comunicações – Tático aos mais baixos escalões (neste caso escalão Pelotão), concluindo-se que a modularidade e a flexibilidade na configuração dos sistemas se revelou como uma mais valia.

Metodologia de Avaliação de Riscos para Cibersegurança com IA em Redes de Missão Federadas

Alferes-Aluno Tm Eduardo Esteves
TPO Transmissões

Resumo - O aumento da sofisticação das ciberameaças, particularmente em ambientes críticos como as Redes de Missão Federadas (FMNs), exige o desenvolvimento de soluções de cibersegurança mais avançadas. A Inteligência Artificial (IA) emergiu como uma ferramenta poderosa na deteção e mitigação de ataques complexos. Contudo, o uso de IA nestes ambientes sensíveis introduz um conjunto próprio de riscos. Este documento apresenta uma metodologia abrangente de avaliação de riscos, concebida para avaliar ferramentas de cibersegurança baseadas em IA, especificamente para FMNs. A metodologia identifica, avalia e mitiga sistematicamente os riscos potenciais, integrando métodos como OWASP e STRIDE. Este documento demonstra a eficácia da metodologia através de avaliações práticas utilizando ferramentas como Demisto (Cortex XSOAR) e Cortex XDR, entre outras, destacando pormenores críticos para assegurar a resiliência da rede e a segurança operacional em FMNs.

Introdução

Com o rápido avanço dos ciberataques, as organizações necessitam de mecanismos de segurança sofisticados para proteger infraestruturas sensíveis. As FMNs, que envolvem colaboração entre múltiplas organizações, como operações militares e agências governamentais, são especialmente vulneráveis a ameaças sofisticadas. A dependência de IA para deteção de intrusões, análise de ameaças e automação de respostas está a crescer nas FMNs devido à sua capacidade de analisar grandes volumes de dados em tempo real e de se adaptar a ameaças em evolução.

Todavia, os sistemas de IA introduzem também riscos próprios, incluindo vulnerabilidades associadas a algoritmos de aprendizagem automática, integridade de dados e potenciais ataques adversários. Este documento propõe uma metodologia de avaliação adaptada às ferramentas baseadas em IA nas FMNs. A estrutura integra o método de avaliação de riscos OWASP com o modelo de ameaças STRIDE para assegurar uma avaliação robusta das ferramentas de IA. Apresentamos também aplicações práticas da metodologia, aplicando-a a ferramentas como o Cortex XDR, uma plataforma abrangente de deteção e resposta a ameaças habilitada por IA, e o Demisto (Cortex XSOAR), uma plataforma SOAR que integra dados de diversas ferramentas de segurança para simplificar fluxos de trabalho de resposta a incidentes.

Estado da arte

Inteligência Artificial na Cibersegurança

A IA desempenha um papel transformador na cibersegurança, implementando algoritmos de aprendizagem automática (ML) que permitem aos sistemas aprender com os dados, adaptar-se a novos padrões e fazer previsões em tempo real. A IA é particularmente eficaz na análise de grandes conjuntos de dados, como registos de tráfego de rede, e na identificação de anomalias que indicam comportamentos maliciosos [1].

A aprendizagem supervisionada baseia-se em dados rotulados para treinar modelos de IA, que são então utilizados para classificar e prever eventos futuros. Por outro lado, a aprendizagem não supervisionada identifica padrões ocultos nos dados sem etiquetas explícitas, tornando-a altamente eficaz para a deteção de anomalias em aplicações de cibersegurança. A aprendizagem por reforço, outro paradigma crítico de IA, utiliza ciclos de feedback para permitir que os sistemas aprendam com as suas ações, melhorando ainda mais as suas capacidades de tomada de decisão.

Embora as ferramentas de IA melhorem a eficácia das defesas cibernéticas, também introduzem novas vulnerabilidades. Ataques adversários a modelos de IA, onde os atacantes manipulam dados de entrada para enganar o sistema, podem levar a falsos negativos ou positivos na deteção de ameaças. Garantir que os modelos de IA permaneçam robustos contra esses ataques é crucial para a cibersegurança baseada em IA.

Redes de Missão Federadas

As Redes de Missão Federadas (FMNs) são redes altamente colaborativas que envolvem múltiplos intervenientes, como forças militares aliadas, agências governamentais e outras organizações. Estas redes requerem elevados níveis de segurança, interoperabilidade e integridade de dados para funcionarem de forma eficaz. Os desafios de segurança nas FMNs são únicos devido à sua escala, à sensibilidade dos dados e à necessidade de comunicação integrada entre diferentes entidades [2].
As ferramentas de cibersegurança habilitadas por IA, incluindo Sistemas de Deteção de Intrusões (IDS) e plataformas de Orquestração, Automação e Resposta de Segurança (SOAR), estão a ser cada vez mais utilizadas nas FMNs para proteger contra ameaças potenciais. Contudo, a implementação destas ferramentas em FMNs introduz novos riscos, especialmente no que diz respeito à capacidade da IA para lidar com protocolos de comunicação diversos e cenários de ameaças variados.

Trabalhos Relacionados

Cibersegurança com IA

A integração da IA na cibersegurança tem sido amplamente estudada nos últimos anos, com foco na melhoria da deteção de intrusões, deteção de *malware* e capacidades de gestão de riscos. A investigação demonstra que os sistemas habilitados por IA podem melhorar significativamente a precisão na deteção de ameaças, identificando padrões que os sistemas baseados em regras tradicionais podem não conseguir detetar. No entanto, persistem desafios significativos em garantir que os sistemas de IA sejam seguros, explicáveis e livres de preconceitos que possam afetar os seus processos de tomada de decisão.

Os Sistemas de Deteção de Intrusões (IDS) são uma das principais aplicações da IA na cibersegurança [3]. Os IDS tradicionais dependem de deteção baseada em assinaturas, que compara padrões de ataques conhecidos. No entanto, os IDS potenciados por IA conseguem detetar ameaças anteriormente desconhecidas, aprendendo com o tráfego de rede e identificando anomalias. Apesar do seu potencial, os IDS baseados em IA são vulneráveis a ataques adversários, em que entradas maliciosas são concebidas para evitar a deteção.

Gestão de Riscos em Ferramentas com IA

Metodologias de gestão de riscos, como OWASP e STRIDE, foram adaptadas para avaliar ferramentas habilitadas por IA. Contudo, a maioria dos *frameworks* existentes não aborda adequadamente os desafios únicos impostos pela IA em ambientes críticos, como as FMNs, onde os riscos são mais elevados e a complexidade das interações de rede é maior.

A metodologia desenvolvida neste estudo integra dois métodos-chave: o Método de Classificação de Riscos OWASP e o Modelo de Ameaças STRIDE. Esta integração permite uma avaliação abrangente de riscos gerais de cibersegurança e vulnerabilidades específicas da IA.

.

Metodologia Proposta de Avaliação

Método de Classificação de Riscos OWASP

O Método de Classificação de Riscos OWASP é amplamente utilizado para avaliar vulnerabilidades de software e priorizar estratégias de mitigação de riscos. É estruturado em seis etapas principais [4]:

1. Identificação de Riscos: Documentação de vulnerabilidades de software e riscos potenciais.
2. Estimativa de Probabilidade: Avaliação da probabilidade de uma vulnerabilidade ser explorada.
3. Estimativa de Impacto: Análise das potenciais consequências de um ataque bem-sucedido.
4. Determinação da Severidade do Risco: Combinação de probabilidade e impacto para priorizar os riscos.
5. Decisão sobre o que corrigir: Alocação de recursos com base na severidade dos riscos identificados.
6. Personalização do Modelo de Classificação de Riscos: Ajuste do modelo para satisfazer as necessidades da organização.

Modelo de Ameaças STRIDE

O STRIDE é um método de modelagem de ameaças que categoriza as ameaças em seis tipos principais [5]:

1. Falsificação de Identidade (Spoofing): Ameaças onde um atacante se faz passar por outro utilizador ou entidade para obter acesso não autorizado ou enganar o sistema.
2. Adulteração (Tampering): Ameaças que envolvem modificações não autorizadas de dados ou componentes do sistema.
3. Repudiação (Repudiation): Ameaças associadas à incapacidade de verificar ou autenticar ações ou eventos, dificultando a responsabilização.
4. Divulgação de Informação (Information Disclosure): Ameaças que envolvem acesso não autorizado ou exposição de informações sensíveis.
5. Negação de Serviço (Denial of Service): Ameaças que visam interromper ou degradar a disponibilidade ou funcionalidade de um sistema.
6. Elevação de Privilégios (Elevation of Privilege)}: Ameaças que envolvem a obtenção não autorizada de níveis mais altos de acesso no sistema.

Passos para a Aplicação da Metodologia

O núcleo da metodologia de avaliação de riscos desenvolvida está estruturado em cinco passos principais:

1. Descrever o Papel da Ferramenta de IA na FMN: Definir o propósito e a funcionalidade da ferramenta de IA dentro da FMN. Isto inclui detalhar como a ferramenta se integra na infraestrutura de cibersegurança da FMN e o seu papel esperado na melhoria da segurança da rede.
2. Avaliar como a Ferramenta de IA pode Introduzir Vulnerabilidades Utilizando STRIDE: Avaliar sistematicamente como a ferramenta de IA pode introduzir vulnerabilidades, categorizadas pelos tipos de ameaças definidos no STRIDE.
3. Estimar a Probabilidade de Exploração das Vulnerabilidades Identificadas (OWASP - Passo 2): Considerar a complexidade do ataque, métodos conhecidos de exploração e nível de sofisticação necessário.

Neste passo, adotou-se a seguinte tabela para definir a probabilidade de exploração das vulnerabilidades:

TABELA 1

Escala de Probabilidade de Exploração de Vulnerabilidades Identificadas

Escala	Descrição	Critérios
1	Muito Baixa	• Exploração requer um esforço significativo ou ocasiões raras • Não existem exploits públicos • Apenas atacantes avançados com recursos específicos conseguem explorar a vulnerabilidade
2	Baixa	• Exploração é tecnicamente complexa, mas fazível • Disponibilidade de exploits públicos limitada • Requer um atacante com algumas capacidades e esforço moderado
3	Moderada	• Exploração requer esforço moderado • Existem exploits públicos e ferramentas que exploram a vulnerabilidade • Atacantes com nível normal de habilidade conseguem suceder em certas condições
4	Alta	• Exploração é direta com esforço mínimo • Exploits disponíveis e bem documentados publicamente
5	Muito Alta	• Exploração é trivial ou consegue ser automatizada • Ferramentas e métodos utilizados recorrentemente exploram a vulnerabilidade com facilidade

4. Avaliar o Impacto da Exploração das Vulnerabilidades (OWASP - Passo 3): Analisar as potenciais consequências de uma exploração bem-sucedida nas operações da FMN.

Neste passo, adotou-se a seguinte tabela para definir o impacto da exploração das vulnerabilidades identificadas:

TABELA 2

Escala de Impacto de Exploração de Vulnerabilidades Identificadas

Escala	Descrição	Critérios
1	Muito Baixo	• Impacto negligenciável da confidencialidade, integridade e disponibilidade da informação • Disrupção mínima das operações da FMN
2	Baixo	• Pequeno Impacto, com degradação temporária dos serviços • Sem impactos de longo-prazo para a organização ou da confidencialidade da informação
3	Moderado	• Impacto significativo nas operações ou sistemas específicos • Exposição limitada de informação sensível ou moderada disrupção de serviços
4	Alto	• Impacto severo com comprometimento de informação sensível ou sistemas críticos • Disrupção prolongada de serviços ou potenciais implicações legais/regulatórias
5	Muito Alto	• Impacto catastrófico, como o comprometimento total dos sistemas de missão críticos • Grande perda de informação sensível, danos na reputação da instituição ou consequências legais/regulatórias sérias

5. Priorizar os Riscos e Desenvolver Estratégias de Mitigação (OWASP - Passo 4): Priorizar os riscos identificados com base na combinação de probabilidade e impacto, desenvolvendo estratégias de mitigação apropriadas.

Resultados

Aplicação da Metodologia a um leque de ferramentas de cibersegurança com IA

A tabela seguinte resume a avaliação de cada ferramenta de cibersegurança habilitada por IA com base na metodologia desenvolvida. Cada ferramenta foi avaliada quanto a vulnerabilidades e riscos em parâmetros-chave, como falsificação de identidade, adulteração, DoS e elevação de privilégios. Para cada parâmetro, a probabilidade e o impacto foram classificados numa escala de 1 a 5, sendo o risco correspondente calculado através da multiplicação desses valores. O risco foi ainda categorizado em baixo, médio ou alto, para oferecer uma compreensão clara da gravidade de cada vulnerabilidade ao implementar ferramentas de IA no ambiente das FMNs:

TABELA 3

Probabilidade, Impacto, Risco e Escala de Risco para cada ferramenta IA usando a metodologia desenvolvida

Ferramenta AI	STRIDE	Propabilidade (1-5)	Impacto (1-5)	Risco(L × I)	Escala de Risco
OutGene	Spoofing	3	4	12	Médio
	Tampering	4	5	20	Alto
	DoS	4	5	20	Alto
Cortex XDR	Spoofing	3	4	12	Médio
	Tampering	4	5	20	Alto
	DoS	4	4	16	Alto
	Elevation of Privilege	4	5	20	Alto
Demisto	Spoofing	3	3	9	Baixo
	Tampering	4	5	20	Alto
	Repudiation	3	3	9	Baixo
	DoS	4	4	16	Alto
Phantom	Spoofing	3	3	9	Baixo
	Tampering	4	5	20	Alto
	Information Disclosure	2	4	8	Baixo
	DoS	4	5	20	Alto
	Elevation of Privilege	3	4	12	Médio
DarkTrace	Spoofing	3	4	12	Médio
	Tampering	4	5	20	Alto
	DoS	4	4	16	Alto
Vectra AI	Spoofing	3	3	9	Baixo
	Tampering	4	5	20	Alto
	Elevation of Privilege	3	4	12	Médio
Cynet	Spoofing	3	3	9	Baixo
	Tampering	4	5	20	Alto
	DoS	4	4	16	Alto
Cybereason	Repudiation	3	3	9	Baixo
	Tampering	4	5	20	Alto
	Elevation of Privilege	3	4	12	Médio
Swimlane	Spoofing	3	3	9	Baixo
	Tampering	4	4	16	Alto
	DoS	4	4	16	Alto

Destes valores foi possível verificar que as ferramentas que introduzem menor risco para as FMNs são os SOARs e que os IDS, devido à sua simplicidade, são os que mais risco introduzem na FMN. Também foi possível analisar que o DoS e o *Tampering* são as duas vulnerabilidades que mais impacto causam quando vulnerabilidades deste tipo são exploradas, pelo que devem ser as principais a ter em conta na salvaguarda do bom funcionamento das ferramentas de IA para cibersegurança.

Conclusão

Este estudo oferece uma solução prática e adaptável para avaliar os riscos de ferramentas habilitadas por IA em FMNs. Com a crescente dependência de IA em ambientes críticos, a metodologia proposta serve como um passo significativo na promoção de cibersegurança robusta, alinhando capacidades avançadas de IA com os requisitos rigorosos das FMNs.

Bibliografia

[1] J. Li, "Cyber security meets artificial intelligence: a survey" Frontiers of Information Technology Electronic Engineering, vol. 19, no. 12, p. 1462–1474, Dec 2018.

[2] C. Defence Staff, I. T. Directorate, and D. Ilie, "Achieving interoperability in a federated environment and in the current security context," Romanian Military Thinking, vol. 2022, no. 4, p. 222–235, Dec 2022.

[3] N. Oliveira, I. Praça, E. Maia, and O. Sousa, "Intelligent cyber attack de- tection and classification for network-based intrusion detection systems," Applied Sciences, vol. 11, no. 4, p. 1674, Feb 2021.

[4] OWASP, "Owasp risk rating methodology" https://owasp.org/www-community/OWASP_Risk_Rating_Methodology.

[5] A. Shostack, Threat Modeling: Designing for Security. John Wiley & Sons, 2014.

Integração de um Veículo Não Tripulado Comercial no Sistema de Comunicações do Exército

Alferes-Aluno Tm João Silva
TPO Transmissões

Resumo - Com a crescente evolução do campo de batalha, as vantagens da utilização de plataformas de Veículos Não Tripulados (UxV) em ambientes ou tarefas perigosas para os militares estão a tornar-se cada vez mais evidentes. Os UxVs reduzem a exposição humana ao perigo em ambientes de alto risco. Assim sendo, é importante que as principais informações do veículo possam ser vistas pelos comandantes na Common Operational Picture (COP).

Este estudo explora a integração de UxVs comerciais em operações militares, centrando-se na melhoria da comunicação entre estes veículos e os seus centros de controlo. A solução desenvolvida foi implementada com recurso ao UGV LAFVIN, tendo os testes sido realizados com o apoio da Equipa de Projeto SIC-T. Após a obtenção dos resultados, foi possível retirar valores e conclusões importantes relativamente à utilização de rádios militares — P/PRC-525 e TR5000H — para a integração de um UGV no Battlefield Management System (BMS).

Introdução

A vida humana não tem preço e a perda de vidas pode ser reduzida consideravelmente com a utilização de sistemas autónomos nas Forças Armadas. Atualmente, quase todas as organizações militares utilizam robôs para executar tarefas perigosas em ambientes de alto risco [1]. Um UxV é um veículo que funciona sem um humano a bordo, controlado remotamente ou de forma autónoma. Existem vários tipos de UxVs: Veículo Terrestre Não Tripulado (UGV), Veículo Aéreo Não Tripulado (UAV) e Veículo Marítimo Não Tripulado (UMV) [2].

Nos últimos anos, face ao aumento das tensões militares a nível mundial, nomeadamente com o início do conflito na Ucrânia em 24 de fevereiro de 2022, tem-se verificado uma notória corrida à tecnologia militar. A Organização do Tratado do Atlântico Norte (OTAN) identificou os sistemas autónomos e as comunicações como tecnologias que terão um papel altamente disruptivo nas próximas duas décadas [3].

Estado da Arte

Os UGVs podem navegar em espaços que seriam perigosos ou inacessíveis para os seres humanos e podem operar em ambientes cada vez mais complexos através da inteligência e da eficiência. Ao equipar um UGV com uma câmara ou outros sensores, os operadores podem analisar rapidamente objetos e regiões de interesse com precisão [4].

A. Compressão e transmissão de vídeos

Ao pilotar um UGV, a transmissão de vídeo torna-se um aspeto de extrema importância. O principal problema desse tipo de transmissão é a alta demanda de largura de banda, o que torna a compressão de vídeo muito importante. Esta ação visa disponibilizar a transmissão de vídeo a uma baixa taxa de bits, preservando uma qualidade de imagem satisfatória, neste caso, para a pilotagem do UGV [5].

B. Tecnologias de radiocomunicação aplicadas a UGVs comerciais

A utilização de Wi-Fi para comandar e controlar UxVs oferece várias vantagens que aumentam a eficiência e a flexibilidade operacionais. Um dos principais benefícios é a capacidade de estabelecer uma ligação robusta e de elevada largura de banda, que suporta a transmissão de grandes quantidades de dados, como vídeo e telemetria complexa, em tempo real [6].

As redes celulares são constituídas por várias estações de base, cada uma delas dedicada à transmissão e receção sem fios de dados numa ou mais "células". A forma específica como as bandas de radiofrequência são utilizadas nas telecomunicações móveis é designada por norma sem fios [7].

O *MAVLink* é um protocolo de *middleware* que constitui uma linguagem universal para sistemas autónomos. As mensagens *MAVLink* são formatadas em código binário com um cabeçalho compacto de 8 *bytes*, o que as torna altamente eficientes. Os mecanismos de controlo de erros incorporados asseguram a integridade dos dados [8].

C. BMS

O BMS integra o Sistema de Informação para o Comando e Controlo do Exército (SICCE) do SIC-T, que por sua vez suporta o Comando e Controlo (C2). O BMS funciona através da rede rádio na banda de *Very High Frequency* (VHF) em modo seguro (SECOM-V). Este sistema de C2 foi concebido para unidades de baixa escalão (Batalhão e inferiores) em uso veicular, com uma aplicação que facilita a partilha da posição geográfica no terreno através de terminais portáteis ligados a uma rede rádio segura [9].

O BMS cumpre os requisitos da OTAN, garantindo a interoperabilidade com os meios de comunicação dos países membros da aliança através da norma *Standardization Agreement* (STANAG) 5527 - *Friendly Force Tracking* [10].

D. Rádios Táticos do Exército

O Rádio Tático P/PRC-525 resulta de uma parceria entre a EID e a Rohde & Schwarz. Opera em Alta Frequência (HF), VHF e Ultra Alta Frequência (UHF) e segue a filosofia de Rádio Definido por *Software* (SDR) [9]. Em agosto de 2019, para atender as necessidades do Exército, foram adquiridos rádios TR5000 da família SOVERON da Rohde & Schwarz, nas versões veicular e manpack, TR5000V e TR5000H [11].

Solução para a Integração de um UGV Comercial no Sistema de Comunicações do Exército

Para a comunicação sem *hardware* de piloto automático, foram utilizadas duas arquiteturas: uma com comunicação Wi-Fi, e outra utilizando *Combat-Net Radio* (CNR), representada na Figura 1, para esta implementação foi utilizado o LAFVIN Multi-Functional Smart Car Kit. A ligação *Raspberry Pi* ↔ Arduino foi concebida para enviar os comandos de controlo recebidos pelo Raspberry Pi para o Arduino. A ligação *Raspberry Pi* ↔ *GCS* foi concebida para enviar os comandos de controlo para o *Raspberry Pi* e o *GPS* e a imagem para a GCS.

A Figura 1 apresenta o cenário com um rádio ligado ao UGV. Este cenário faz sentido quando o UGV é capaz de transportar um rádio. Nesta aplicação específica, o UGV LAFVIN não é utilizado com um rádio veicular em testes em movimento, dado que, devido à sua dimensão, só pode ser utilizado em testes estáticos ou com rádios de pequenas dimensões. Em situações sem rádio, todas as comunicações com o UGV são efetuadas via Wi-Fi.

Na comunicação com CNR, o computador da GCS e o *Raspberry Pi* ligam-se ao rádio através de um cabo de rede. A antena utilizada depende da versão do rádio — *manpack* ou veicular. No lado da GCS, o *gamepad* liga-se ao computador por USB; no lado do UGV, o GPS liga-se ao *Raspberry Pi* por USB. Por outro lado, o Raspberry Pi e a câmara são ligados através de um Circuito Impresso Flexível (FPC). O Arduino liga-se ao *Raspberry Pi* através de um cabo de série.

Na comunicação Wi-Fi, todas as ligações são utilizadas, exceto as dos rádios táticos, uma vez que a tecnologia Wi-Fi é utilizada para a comunicação, que é feita através das placas de rede integradas em cada dispositivo (computador GCS e *Raspberry Pi*).

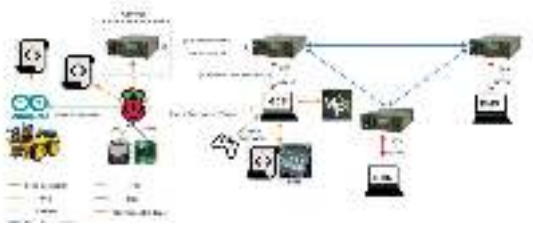


Figura 1: Arquitetura Geral — Wi-Fi + Rádios Militares

A. Arquitetura GCS

O *software GCS MAVProxy* estabelece uma ligação com o *Raspberry Pi.* O sistema GCS é um servidor *proxy* entre o *Raspberry Pi*, o *Mission Planner* e o BMS. A arquitetura da GCS tem de ser assim para que os dados possam ser enviados/recebidos simultaneamente para o BMS e para o *Mission Planner*. Esta arquitetura também permite filtrar as mensagens enviadas para cada um dos programas. No caso da comunicação com CNR, uma vez que existe um cenário de comunicação híbrida, em que alguns dados são enviados via Wi-Fi e outros via rádios militares, foram estabelecidas duas ligações entre o *Raspberry Pi* e o MAVProxy que corre na GCS.

B. Pilha de Protocolos

A pilha de protocolos para comunicação sobre Wi-Fi consiste numa pilha TCP/IP convencional. A camada de transporte será TCP/UDP, e a camada de Rede será IP; as camadas Física + Ligação correspondem aos protocolos Wi-Fi. Relativamente à comunicação sobre os rádios táticos P/PRC-525 e TR5000 é de salientar que este possui um módulo de encaminhamento *Mobile Ad Hoc Network* (MANET) na camada de rede. Tal como na comunicação Wi-Fi, a camada de transporte é TCP/UDP e a camada de Rede é IP. As camadas Física + Ligação correspondem a protocolos específicos do rádio.

C. Componentes de Hardware

Uma vez que o *Raspberry Pi 3 Model B+* já era um recurso existente, dado o seu baixo preço e já ser utilizado em muitas implementações idênticas, a escolha recaiu sobre este, poupando recursos. Como o objetivo era controlar o veículo através do Mission Planner, não foram utilizados os sensores do *kit LAFVIN*; apenas foram utilizados o Arduino UNO, a placa de expansão V5, 4 motores DC e a placa de motores L298N. O UGV ficou assim constituído pelos seguintes componentes:

1. *Raspberry Pi 3 Model B+*;
2. *Kit LAFVIN*;
3. Bateria;
4. G-Mouse GPS VK-162;
5. *Raspberry Pi Camera Module 2*;
6. Rádio.

A utilização de um rádio militar no UGV é apenas para comunicação com CNR e depende do peso e do volume do rádio, tendo em conta a capacidade de carga útil do UGV. A GCS é constituída pelos seguintes componentes:

1. Computador;
2. *Gembird Gamepad*;
3. Rádio.

Tal como no UGV, os rádios militares são utilizados na GCS apenas para comunicação com CNR. É importante notar que, neste estudo, a câmara utilizada para a transmissão é do mesmo fabricante que a unidade de bordo. Este facto facilita a integração da câmara com a unidade de bordo; apenas é necessário configurar a câmara nas definições, sem necessidade de *software* específico.

D. Módulos de Software

Foram desenvolvidos três *scripts* de *software*. O software desenvolvido foi também integrado com o *software* de GCS. O bloco de *delay* na lógica de envio de *heartbeats* permite o controlo da frequência de envio de mensagens HEARTBEAT. O bloco de *delay*, na lógica de envio da posição, presente em ambos os *scripts*, permite ajustar a frequência de envio de mensagens de posição, GPS_RAW_INT no caso da Figura 2 (Script 1), e de mensagens XML para o BMS com a identificação do UGV e a sua posição, no caso da Figura 2 (Script 2). Este ajuste de frequência permite comunicar em cenários com menor largura de banda disponível.

O código do fabricante do LAFVIN UGV, representado pelo *Script* 0 na arquitetura geral, teve de ser adaptado, uma vez que a comunicação é agora feita através de um cabo de série, e o fabricante não prevê este modo de comunicação. No Arduino, a função *processRaspberryPiCommand*(String command) permite a receção de comandos através de uma ligação série ao *Raspberry Pi*. Para evitar problemas, todos os outros modos de comunicação — Infravermelhos e *Bluetooth* — foram desativados.

O *Script* 1, apresentado na Figura 2, representa uma ligação entre o UGV e a GCS utilizada para enviar a posição do UGV para a GCS. Também é utilizado para enviar comandos de controlo para o UGV. Este *script* é executado no *Raspberry Pi*. No caso da comunicação via rádios militares, é necessário iniciar duas ligações ao MAVProxy, uma para os rádios e outra para a Wi-Fi, uma vez que ambos são utilizados.

Para obter a posição do UGV, foram utilizadas as bibliotecas "gpsd", "gpsd-clients" e "python-gps" para obter os dados GPS utilizando a função *get_gps_data()*. Estas bibliotecas foram instaladas no *Raspberry Pi*. O passo inicial é iniciar a sessão, e depois as variáveis latitude, longitude e altitude são atualizadas em tempo real. Depois de ter as variáveis a atualizar, foi criada a função *send_position*(latitude, longitude, altitude). Esta função envia mensagens MAVLink GPS_RAW_INT com dados de latitude, longitude e altitude para o *Mission Planner*.

As mensagens MAVLink MANUAL_CONTROL são recebidas pelo Raspberry Pi utilizando a função *handle _manual_control*. Em função dos parâmetros recebidos, a mensagem correspondente é enviada ao Arduino para acionar o UGV. Para enviar comandos de controlo para o UGV, o *Gembird Gamepad* foi primeiro ligado à GCS e depois emparelhado com o *Mission Planner*.

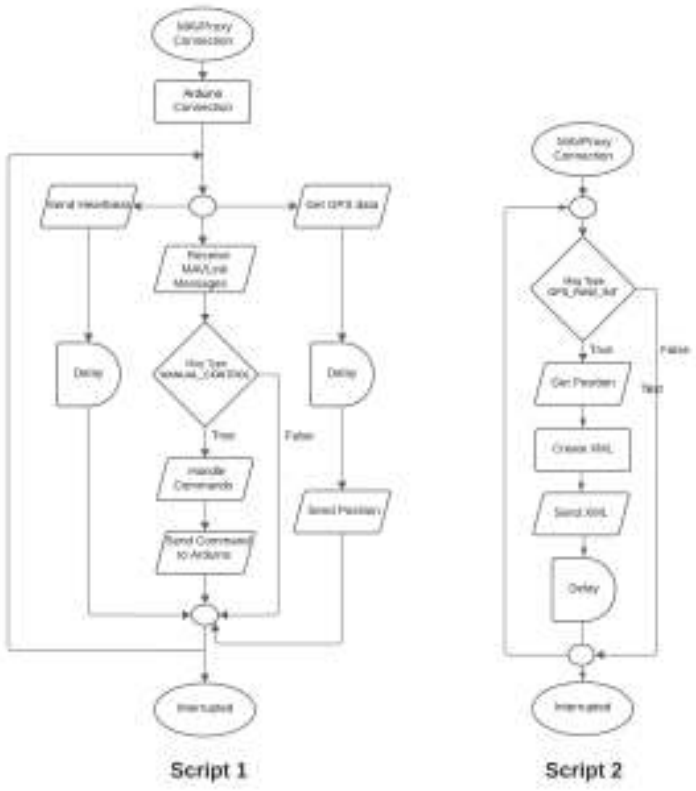


Figura 2: Script 1 e Script 2

O *Script* 2, apresentado na Figura 2, é executado na GCS e representa uma ligação ao BMS. Cria um XML, que é enviado para o BMS. Este *script* tem por objetivo extrair a posição do UGV das mensagens MAVLink e gerar um XML de acordo com o STANAG 5527. A ligação é estabelecida com a porta 14552, para onde as mensagens MAVLink são reencaminhadas através do MAVProxy. Este script pode ser executado na GCS se o MAVProxy estiver a encaminhar mensagens para a porta 14552 do *localhost* ou noutra máquina. No cenário com CNR, este envio é feito através de rádios militares.

O *IP* para onde é enviada a posição deve ser configurado na função *send_xml_file(filename, server_ip, server_port)* utilizada para enviar o ficheiro XML. No BMS, para além da configuração padrão, que inclui a criação de uma missão com alguns parâmetros obrigatórios, como a configuração da pilha e do GPS, deve ser configurado no BMS um *gateway* com a porta onde será recebido o relatório XML, neste caso a porta 48882, e o modelo de mensagem que será utilizado, neste caso o *FFT Systems-STANAG 5527 A1/A2*.

E. Configuração do *Mission Planner*

O *Mission Planner* é configurado na porta 14551; assim que o *software* é aberto, após executar o *Script* 1 e iniciar a GCS com o MAVProxy, é automaticamente iniciada uma ligação UDP na porta 14551. Inicialmente, é apresentada a configuração para a receção de vídeo no *Mission Planner* e a sua captura e envio no *Raspberry Pi*, utilizando as bibliotecas *Raspivid e GStreamer*, respetivamente.

F. Transmissão de vídeo

A captura de imagem foi inicialmente realizada utilizando a aplicação *Raspivid* no *Raspberry Pi*. Posteriormente, a aplicação *GStreamer* foi utilizada para enviar o fluxo de vídeo ao *Mission Planner*, em execução na GCS. A qualidade da captura de imagem tem influência na largura de banda necessária para a comunicação. A qualidade da imagem é ajustada de acordo com as características do canal de transmissão, que serão analisadas nos resultados.

Resultados

Os testes realizados com apoio da equipa do projeto SIC-T, incluem o uso exclusivo de Wi-Fi e uma configuração híbrida com rádios táticos e Wi-Fi. Os rádios táticos foram usados de forma a obter comunicação segura, dado que a posição do UGV é um dado crítico. A solução consistiu em gerar e enviar ficheiros XML com a posição do UGV para o BMS. Isto foi realizado utilizando o *Script* 2 e pode ser enviado via Wi-Fi, rádios militares ou outra tecnologia *IP*.

Os testes Wi-Fi foram divididos entre o uso de uma infraestrutura de rede existente e a arquitetura *RAD-MAVLink-Bridge*, que transforma o *Raspberry Pi* num ponto de acesso sem fios. Nos testes com rádios militares, foram avaliados os rádios P/PRC-525 e TR5000H. O computador usado na GCS corria Windows 11 com Ryzen 7 e 16 GB RAM; os computadores simbolizados por BMS, eram *Getac* a correr Windows 10 Pro com Intel Core i5 e 8 GB RAM.

A. Cenário 1: Wi-Fi

Nos testes com Wi-Fi, todos os dados foram enviados utilizando Wi-Fi 4 (802.11n) a 2,4 GHz. A GCS e o *Raspberry Pi* precisavam apenas de estar na mesma rede, representado pela Figura 3.

Figura 3: Arquitetura de Rede — Wi-Fi

O BMS pode ser executado na GCS, enviando o XML para o *localhost* via TCP. O *Script* 2 era necessário em ambos os casos.

B. Cenário 2: Wi-Fi-RAD-MAVLink-Bridge

A biblioteca *RAD-MAVLink-Bridge* transforma o *Raspberry Pi* num ponto de acesso sem fios (*rad--bridge*). O protocolo usado é o Wi-Fi 4 (802.11n) a 2,4 GHz. A arquitetura foi semelhante à do cenário anterior, mas a rede era gerada diretamente no *Raspberry Pi*.

C. Cenário 3: Rádios Militares — P/PRC-525

Neste cenário, os rádios P/PRC-525 foram usados para enviar mensagens críticas (*HEARTBEAT, GPS_RAW_INT e XML*) por VHF (102-104 MHz) em IPoA, representado pela Figura 4.

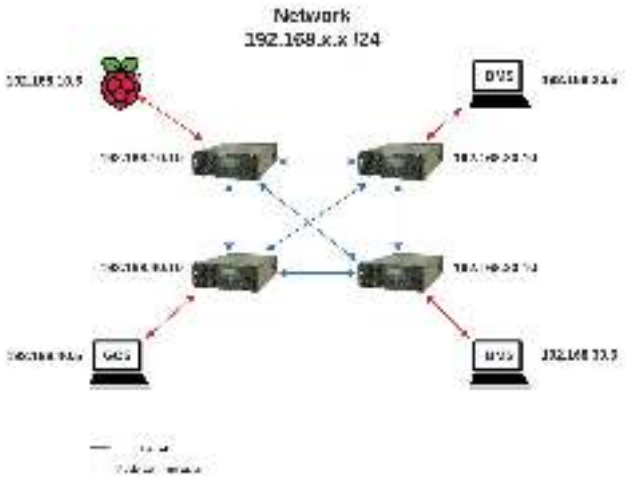


Figura 4: Arquitetura de Rede — P/PRC-525

O vídeo e os comandos de controlo foram enviados por Wi-Fi. Estes testes foram feitos num cenário estático, dadas às limitações de *payload* do UGV.

D. Cenário 4: Rádios Militares — TR5000H

Com os rádios TR5000H, foi utilizada comunicação por VHF (225-228 MHz) em IPoA. As mensagens críticas (HEARTBEAT, GPS_RAW_INT e XML) foram enviadas por rádio, enquanto o vídeo e comandos de controlo continuaram a ser enviados por Wi-Fi. Esta configuração destacou-se pelo controlo automático do tráfego e pela possibilidade de comunicação simultânea de voz e dados.

E. Avaliação da Solução

Os resultados de desempenho foram obtidos com o iPerf3, configurando o *Raspberry Pi* como servidor e a GCS como cliente. Os testes incluíram medições de *throughput* TCP, largura de banda bidirecional TCP e testes UDP para jitter e perdas de dados.
Nos testes com Wi-Fi, houve degradação de desempenho em cenários dinâmicos, com taxa de transferência de 19,1 Mbit/s em condições estáticas. A configuração *Wi-Fi-RAD-MAVLink-Bridge* mostrou boa performance a curtas distâncias, mas com degradação significativa além de 40 metros. Nos testes com rádios militares, o TR5000H demonstrou maior eficiência ao controlar automaticamente o tráfego, não dando primazia ao envio de dados UDP, contrariamente ao cenário com o P/PRC-525.

Conclusões

Este estudo desenvolveu a primeira arquitetura para integração de UxVs no BMS, permitindo o comando de um UGV sem *hardware* de piloto automático específico. Os testes com Wi-Fi mostraram que, mesmo com baixa largura de banda, a comunicação era mantida, havendo alguma degradação no envio de vídeo. A configuração *RAD-MAVLink-Bridge* é adequada para curtas distâncias e pode ser melhorada com antenas direcionais. Os rádios militares permitiram comunicação segura, mas apresentaram limitações de largura de banda. O TR5000H mostrou-se superior ao P/PRC-525, com melhor gestão de tráfego e comunicação paralela. Futuras melhorias podem incluir mais cenários de teste e frequências utilizadas, além de configurações otimizadas para dar prioridade a dados críticos.

Referências bibliográficas

[1] H. Saputra and M. Mirdanies, "Controlling Unmanned Ground Vehicle Via 4 Channel Remote Control," Energy Procedia, vol. 68, 04 2015.

[2] J. Chen, J. Sun, and G. Wang, "From unmanned systems to autonomous intelligent systems," Engineering, vol. 12, pp. 16–19, 2022.

[3] N. S. T. Organization, "Science & Technology Trends 2023-2043 Across the Physical, Biological, and Information Domains," 2023.

[4] B. Hament and P. Oh, "Unmanned aerial and ground vehicle (UAV-UGV) system prototype for civil infrastructure missions," in 2018 IEEE International Conference on Consumer Electronics (ICCE), 2018, pp.1–4.

[5] B. Sivam, S. M G, and P. Sreelatha, "Survey on video compression techniques for efficient transmission," Journal of Physics: Conference Series, vol. 1916, p. 012211, 05 2021.

[6] J. Ge, T. Li, and T. Geng, "The wireless communications for unmanned surface vehicle: An overview," in Intelligent Robotics and Applications, Z. Chen, A. Mendes, Y. Yan, and S. Chen, Eds. Cham: Springer International Publishing, 2018, pp. 113–119.

[7] I. Prlíc, J. Sisko, V. Varnai, L. Pavelic, J. Macan, S. Kobescak, M. Ha-jdinjak, M. Jurdana, Z. Cerovac, B. Zauner, M. Mihic, and S. Avdagíc, "Wi-Fi technology and human health impact: A brief review of current knowledge," Archives of Industrial Hygiene and Toxicology, vol. 73, pp.94–106, 06 2022.

[8] MAVLink, "MAVLink Common Messages," 2024, acedido: 2024-08-14. [Online]. Disponível: https://mavlink.io/en/messages/common.html.

[9] V. Sequeira, "Sistema de Comando e Controlo BMS - Battlefield Management System," Revista Militar da Brigada Mecanizada - Atoleiros, vol. 34, pp. 54–57, 04 2020.

[10] North Atlantic Treaty Organization, "STANAG 5527: Friendly Force Tracking," NATO, Washington, D.C., USA, Tech. Rep., 2017.

[11] R. de Transmissões, "Revista Mensagem 2021," Regimento de Transmissões, 03 2021, Boletim Informativo do Regimento de Transmissões.

Aplicação de energias renováveis a sistemas de contentores militares

Alferes-Aluno Tm Simão Neves
TPO Transmissões

Resumo- A aplicação de energias renováveis está a tornar-se cada vez mais comum em diversas áreas, incluindo no contexto militar. Este trabalho tem como objetivo integrar as energias renováveis em sistemas de contentores militares, visando a produção de energia para autoconsumo e, consequentemente, a redução da dependência de combustíveis fósseis. O presente trabalho inicia com uma revisão abrangente da literatura sobre as três principais fontes de energias renováveis: solar, eólica e hidráulica, seguida da apresentação das aplicabilidades e características específicas dos sistemas de contentores militares. Também foi realizada uma investigação em relação ao envolvimento de Portugal em diversas regiões do mundo. Quanto ao estado da arte, o objetivo deste capítulo é apresentar diferentes estudos realizados no contexto da aplicação de energias renováveis em sistemas de contentores militares, com ênfase na implementação de sistemas híbridos de energia para esses contentores. Na metodologia adotada para este estudo inicialmente são definidos os métodos e ferramentas necessários para alcançar os resultados pretendidos. Foram projetados dois sistemas híbridos para duas localizações distintas: República Centro-Africana e Roménia. Os resultados obtidos demonstram que a incorporação de energias renováveis a sistemas de contentores militares é economicamente e ambientalmente vantajosa para as Forças Nacionais Destacadas. Estes sistemas não só poderão reduzir custos operacionais, como também aumentar a sustentabilidade e resiliência energética das operações militares.

Introdução

O desenvolvimento de soluções inovadoras alinhadas a práticas sustentáveis é essencial, especialmente no meio militar, onde a adoção de Energias Renováveis (ER) oferece diversas vantagens. As ER, como solar, eólica e hidráulica, são fontes limpas e sustentáveis que podem alimentar sistemas de contentores militares, reduzindo a pegada de carbono, os custos logísticos e os riscos de segurança associados ao transporte de combustíveis. Além disso, elas garantem maior eficiência operacional, viabilizando operações ininterruptas e sustentando equipamentos essenciais, como sistemas de comunicação e iluminação. A aplicação de ER em locais remotos, onde a energia elétrica é escassa, destaca sua importância para a sustentabilidade e eficiência das operações militares.

Metodologia

O trabalho tem como principal objetivo explorar as aplicações das ER em sistemas de contentores militares, apresentando uma abordagem inovadora e estratégica para maximizar a eficiência operacional e fomentar a sustentabilidade nas Forças Nacionais Destacadas. Neste capítulo, serão apresentadas as metodologias utilizadas para garantir que o objetivo do trabalho seja alcançado. Serão descritas as diversas tarefas envolvidas no projeto, os passos a serem seguidos para o desenvolvimento de cada uma, bem como as ferramentas necessárias para a obtenção dos resultados.

A. Painéis Solares

As células solares que irão ser alvo de análise são as do 1M3P. A corrente de saída, I, pode ser calculada em função da tensão de saída, V, através da seguinte equação [1], [2]:

onde a corrente do díodo é dada por:

$$I = I_{fv} - I_d \quad (1)$$

$$I_d = I_o\left(e^{\frac{V}{bV_T}} - 1\right) \quad (2)$$

sendo Ifv a corrente fotovoltaica, b o fator de não idealidade do díodo, Io a corrente de saturação do díodo, VT correspondente à tensão térmica que pode ser calculada através da equação 3, onde T é a temperatura, k a constante de Boltzmann e q o módulo da carga do eletrão:

$$V_T = \frac{kT}{q} \quad (3)$$

Para calcular a potência de saída, P, é necessário multiplicar o valor de V, com o valor de I. Esta potência não está relacionada com a potência máxima (MPP) que a célula é capaz de produzir. O MPP corresponde ao momento em que a derivada parcial da potência P em ordem a V é nula.

Os fatores com maior influência no rendimento das células solares são a temperatura e a irradiância. De modo a analisar a sua preponderância, é fundamental assumir que [1]:

• O fator de não idealidade do díodo, b, mantém-se inalterado;

• A corrente de saturação do díodo, Io , varia apenas com a temperatura, tal que:

$$I_o(T) = I_o^r\left(\frac{T}{T^r}\right) e^{\frac{E_g}{b}\left(\frac{1}{V_T^r} - \frac{1}{V_T(T)}\right)} \quad (4)$$

• A corrente fotovoltaica que é aproximadamente igual à corrente de curto-circuito, Icc , varia apenas com a irradiância, G.

$$I_{cc} = \frac{G}{G^r} I_{cc}^r \quad (5)$$

Um painel fotovoltaico é constituído por z células, com m células em série e n células em paralelo. Considerando que todas as células do painel são iguais ao apresentarem um comportamento idêntico, a tensão, a corrente e a potência de saída do painel solar podem ser calculadas através das seguintes equações [1]:

$$V_{\text{Painel}} = m \cdot V_{\text{Célula}} \quad (6)$$

$$I_{\text{Painel}} = n \cdot I_{\text{Célula}} \quad (7)$$

$$P_{\text{Painel}} = z \cdot V_{\text{Célula}} = (m \cdot n) \cdot P_{\text{Célula}} \quad (8)$$

B. Turbinas Eólicas

Serão explorados dois tipos de turbinas eólicas: de eixo vertical e de eixo horizontal. Será necessário analisar as vantagens de cada modelo, considerando diversos fatores, tais como a potência nominal, orientação do eixo, área varrida, Ar, velocidade do vento na qual a turbina é operacional, eficiência da turbina, ηte, e coeficiente de potência, cp.

É importante relembrar que a recolha dos dados destes parâmetros é crucial, uma vez que estes afetam diretamente a produção de energia eólica. A potência total extraída através da turbina eólica pode ser calculada utilizando a seguinte equação:

em que:

$$P_t = P_w \cdot \eta_{te} \quad (9)$$

$$P_W = \frac{\rho_{ar}}{2} c_p(\lambda) A_r v_W^3 \quad (10)$$

A Produção Anual de Energia (PAE), refere-se à totalidade de energia eólica convertida em eletricidade ao longo de um ano. A PAE de uma turbina pode ser determinada integrando a potência para cada cenário de vento registado durante um ano [3]. Este cálculo é realizado através da aplicação da curva de potência da turbina em combinação com a distribuição anual do vento.

$$PAE_t = T_{anual} \int_{\theta 0}^{\theta 360} \int_{v_w 0}^{v_w \infty} P_W(v_W) f_{vw}(v_W) dv d\theta \quad (11)$$

onde Tanual é a duração do ano em horas, θ é a direção do vento, vw0 é a velocidade mínima do vento, vw∞ é a velocidade máxima do vento.

Considerando que todas as turbinas eólicas apresentam um comportamento semelhante, a PAE total do sistema é a soma das PAEs individuais de cada turbina. Esta relação pode ser expressa pela seguinte equação:

$$PAE_{total} = N_t . PAE_t \quad (12)$$

De modo a maximizar o conjunto total das turbinas eólicas, é essencial minimizar os efeitos de turbulência conhecidos como *wake effects*, que resultam do layout e do posicionamento das turbinas. Trata-se de uma pequena interferência no fluxo do vento causada por uma turbina em relação à turbina anterior. Para reduzir estas perdas, a localização e a orientação das turbinas é um fator a considerar.

C. Análise do Terreno e Infraestrutura

Para garantir a eficiência e a adequação do sistema a implementar, a análise do terreno e das infraestruturas terá de ser realizada de forma rigorosa. Para tal, é necessário considerar as suas dimensões e localizações. Além disso, deve-se avaliar a irradiância disponível e a velocidade média do vento.

1. Análise Climatológica

A análise climatológica consiste no estudo detalhado das condições climáticas de uma determinada localização ao longo de um período específico. Esta análise pode abranger diversas variáveis, como temperatura, humidade, irradiância, velocidade do vento e pressão do ar, entre outras. O objetivo é identificar as tendências climáticas da região em estudo. Para este propósito, os dados sobre as condições atmosféricas serão obtidos através da ferramenta PVGIS e do *software* HOMER Pro.

2. Dimensionamento da Carga

Para realizar o dimensionamento do sistema em causa, é necessário conhecer o valor do consumo médio mensal de uma Força Nacional Destacada (FND). Esse valor será inserido num algoritmo desenvolvido em *Python*. O algoritmo recolhe e processa os dados do consumo de modo a aplicar os cálculos necessários para o dimensionamento do sistema.

D. Dimensionamento do Sistema

A avaliação financeira de um sistema é uma etapa importante para a determinação da sua viabilidade económica, incluindo o Retorno sobre o Investimento (ROI) e o Prazo de Retorno do Investimento (PRI). Este processo envolve a análise dos custos e benefícios associados à implementação e operação do sistema, proporcionando uma visão clara sobre a sua eficiência e sustentabilidade financeira. Para realizar esta avaliação, é essencial conhecer os preços dos componentes que irão integrar o gerador híbrido, os custos de manutenção e o potencial ganho financeiro que o sistema irá viabilizar resultante da poupança no consumo de combustíveis fósseis. O ROI é uma métrica que relaciona os benefícios do investimento com os custos associados. O cálculo de ROI é dado pela seguinte equação [4]:

$$ROI = \frac{GFin - CFin}{CFin} \quad (13)$$

em que:

- GFin representa os ganhos financeiros do projeto;
- CFin representa os custos financeiros do projeto.

O PRI é um método que mede o tempo decorrido desde o início do investimento até ao momento em que o investimento é totalmente recuperado [5]. O PRI pode ser obtido utilizando a equação 14.

$$PRI = \frac{I_0}{GP} \quad (14)$$

em que:

- I0 é o investimento inicial do projeto;
- GP é a receita anual.

O gerador híbrido incorpora múltiplas fontes de energia para otimizar a eficiência e a sustentabilidade do sistema. Utiliza painéis solares para capturar a energia solar, turbinas eólicas para aproveitar a energia do vento e um gerador a diesel como *backup*, garantindo um fornecimento contínuo de energia mesmo em condições adversas. Os componentes elétricos e eletrónicos podem ser alimentados por tensão AC ou tensão DC, dependendo das suas especificações e necessidades. No caso de dispositivos que requerem DC, a conversão da energia AC em DC é, geralmente, realizada pelos próprios componentes, dispensando a necessidade de inversores. No entanto, para o fornecimento de energia a cargas que utilizam AC, quando a fonte disponível é DC, é imprescindível o uso de inversores. Estes dispositivos são responsáveis pela conversão de tensão DC em tensão AC, possibilitando a operação adequada dos equipamentos que dependem deste tipo de alimentação.

Para determinar a solução mais eficiente e adequar as fontes de ER ao campo, foi desenvolvido um algoritmo de otimização para calcular a melhor configuração para o projeto. Após obter os resultados, o algoritmo itera sobre diferentes combinações de percentagens de energias solar e eólica, calculando para cada combinação o respetivo ROI. No final deste ciclo de iterações, é selecionada a combinação com o ROI mais elevado. Em seguida, o algoritmo recalculará os resultados para confirmar a solução ótima.

Resultados

No presente capítulo serão demonstrados os resultados obtidos ao longo do desenvolvimento do trabalho através da metodologia apresentada no capítulo anterior.

A. Painéis Solares

O painel solar considerado e disponível para o desenvolvimento deste projeto é o modelo SZ-100-33MF [6] da empresa SolarFam. Este painel é constituído por silício monocristalino (mono-Si) e possui 33 células dispostas em série. Estas são otimizadas para condições de baixa irradiância e incluem díodos bypass, o que permite o funcionamento do painel mesmo em situações de sombreamento parcial, como quando está nublado ou ocorre outro tipo de obstrução, como a queda de folha ou a acumulação de poeiras. Os parâmetros do painel solar SZ-100-33MF [6] podem ser observados na Tabela I.

A_{ativa} (m^2)	Nº de células	I_{cc} (A)	V_{cm} (V)	$P_{máx}$ (W)	η_{cel} (%)	Preço (€)
0,564	33	6,51	19,70	100	19,27	236

Tabela I: Parâmetros do painel solar SZ-100-33MF [6]

B. Turbinas Eólicas

A turbina eólica escolhida para o dimensionamento do sistema foi a Aeolos-V 10kW [7]. Esta turbina foi selecionada por ser uma turbina de eixo vertical, o que elimina a necessidade de alinhar a turbina com a direção do vento. Devido ao seu design de eixo vertical, a turbina ocupa menos espaço, contribuindo significativamente para a otimização do espaço disponível. O modelo possui três lâminas de eixo vertical, cada uma com cerca de 5,5 metros de comprimento. Também possui um travão mecânico responsável por interromper o funcionamento da turbina em situações de manutenção da mesma ou quando a velocidade do vento excede os limites de segurança. Na Tabela II pode-se observar os parâmetros da turbina eólica Aeolos-V 10kW.

P_n (kW)	A_r (m^2)	η_{ts} (%)	C_p	Velocidade do vento de início (m/s)	Preço (Milhares de €)
10	151,18	96	0,24 [8]	2,5	15

Tabela II: Parâmetros da turbina eólica Aeolos-V 10kW [7]

C. Análise da Infraestrutura

O cenário em estudo localiza-se em Bangui, na República Centro-Africana. A escolha deste local deve-se ao facto de ser um Teatro de Operações ativo e pelo clima quente e húmido da sua região. Com o auxílio da ferramenta PVGIS, foi possível determinar o ângulo e o azimute ótimos para a orientação dos painéis solares, maximizando o aproveitamento do gerador solar. O ângulo é de 7º e o azimute de 13º.

Através da ferramenta *Google Earth*, mediu-se a área dos contentores, de alguns telhados das infraestruturas do campo e de uma parte do campo onde poderão ser instaladas as turbinas eólicas. Estas medições possuem uma incerteza de 3,54% [9]. A Figura 1 ilustra as áreas passíveis de instalação dos painéis solares e das turbinas eólicas.

Figura 1: Medição da área disponível para o gerador

A área disponível para a instalação de painéis fotovoltaicos varia entre 6 048 m2 e 6 493 m2, a amarelo, e a azul, para a instalação das turbinas eólicas, está compreendida entre 1 420 m2 e 1 524 m2.

1. Análise Climatológica

Para a análise climática da RCA, foram recolhidas variáveis como a temperatura, a irradiância, a velocidade do vento e a humidade.

2. Dimensionamento da Carga

O campo onde a força está alocada é composto por quatro geradores alimentados a gasóleo. No entanto, apenas dois estão em operação contínua (geradores externos), enquanto os outros dois servem de reserva (geradores internos) em caso de situações de falha ou necessidade de energia extra. O consumo médio por hora é cerca de 110 kWh o que corresponde a um consumo médio diário de 2 640 kWh/dia.
A Figura 2 apresenta o consumo médio por hora do campo na RCA, com base nas variações percentuais do estudo [10].

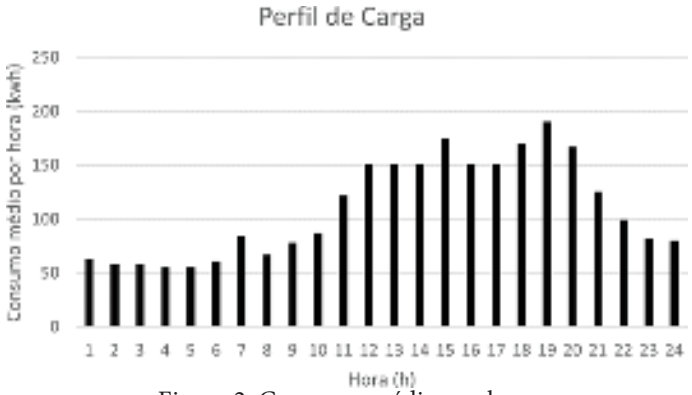


Figura 2: Consumo médio por hora

D. Dimensionamento do Sistema

Com base nos parâmetros apresentados anteriormente e nos restantes valores indicados na Tabela III, foi calculado o dimensionamento ótimo do sistema através do Algoritmo de Otimização. A manutenção anual do sistema corresponde a aproximadamente 1,5% do I0 com base num projeto publicado pela *National Renewable Energy Laboratory* (NREL) [11] e o preço do diesel por litro foi considerado 2€. Os resultados obtidos estão presentes na Tabela IV.

Eficiência máx. do inversor solar (%)	Preço do inversor solar (Milhares de €)	Eficiência máx. do inversor eólico (%)	Preço do inversor eólico (Milhares de €)	Preço dos controladores híbridos (Milhares de €)
98,5	7,25	94	3,5	7

Tabela III: Restantes parâmetros para o dimensionamento do gerador híbrido

Energia solar (%)	100
Energia eólica (%)	0
Nº de painéis solares	1 100
Área total de painéis solares (m^2)	621
Nº de turbinas eólicas	0
J_0(Milhares de €)	277,350
Redução do consumo de *diesel* anualmente (%)	31
Montante economizado anualmente (Milhares de €)	152,309
ROI máximo	276% em 10 anos
PRI mínimo	1 ano e 11 meses

Tabela IV: Resultados do dimensionamento do gerador híbrido

Para esta configuração e localização em análise, foram elaboradas as curvas médias diárias de produção de energia do gerador fotovoltaico e podem ser observadas nas Figuras 3 e 4.

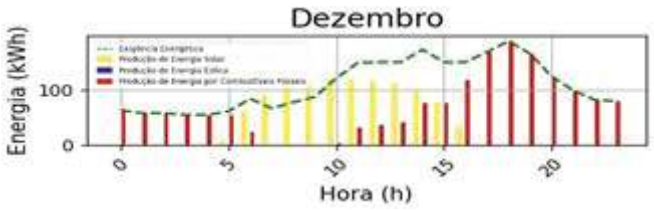


Figura 3: Curva consumo-geração do mês de dezembro na RCA

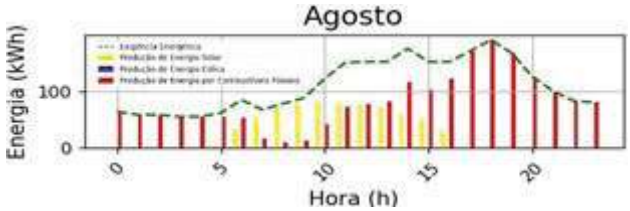


Figura 4: Curva consumo-geração do mês de agosto na RCA

Turbinas eólicas em Bangui são inviáveis devido ao vento inadequado e altos custos. Já os painéis solares são viáveis, pois o telhado disponível acomoda o gerador fotovoltaico necessário, garantindo integração eficiente.

1. Sistema ótimo na Roménia

A escolha da Romênia como local de estudo deve-se ao fato de ser um Teatro de Operações ativo e possuir um clima mais frio, com baixa irradiação solar e ventos mais intensos, contrastando com o clima quente e de alta irradiação da República Centro-Africana (RCA). O sistema previamente dimensionado foi testado na Romênia utilizando o Algoritmo de Otimização, sem adaptações específicas para a região, exceto pela análise climatológica e o preço do gasóleo, considerado em 1,5€/litro. As mesmas variáveis climáticas foram analisadas para a Romênia e a RCA, com os resultados apresentados na Tabela V.

	Sistema dimensionado	Sistema otimizado
Energia solar (%)	100	44
Energia eólica (%)	0	56
Nº de painéis solares	1 100	484
Área total de painéis solares (m²)	621	273
Nº de turbinas eólicas	0	26
I_0 (Milhares de €)	277,350	521,974
Redução do consumo de diesel anualmente (%)	26	62
Montante economizado anualmente (Milhares de €)	95,771	229,305
ROI máximo	200% em 10 anos	282% em 10 anos
PRI mínimo	3 anos	2 anos e 4 meses

Tabela V: Resultados do dimensionamento do gerador híbrido na Roménia

Nas Figuras 5 e 6 é possível observar as curvas de consumo-geração do sistema otimizado implementado na Roménia para os meses de dezembro e agosto.

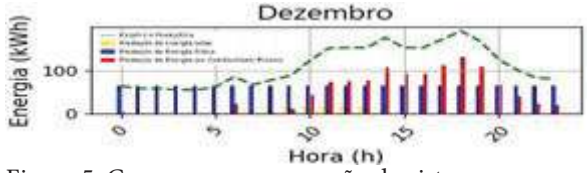


Figura 5: Curva consumo-geração do sistema otimizado para o mês de dezembro na Roménia

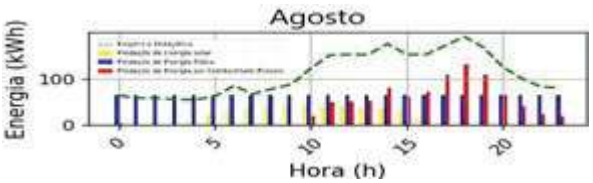


Figura 6: Curva consumo-geração do sistema otimizado para o mês de agosto na Roménia

Conclusão

A integração de ER no meio militar melhora a sustentabilidade, eficiência e autonomia operacional das FNDs. Este estudo demonstrou que sistemas híbridos solares e eólicos reduzem custos, dependência de combustíveis fósseis e logística, sendo viáveis em diferentes cenários. A adaptação de contentores militares para ER destaca sua flexibilidade, aumentando a resiliência e segurança energética.

Referências

[1] R. A. Marques Lameirinhas, J. P. N. Torres & J. P. de Melo Cunha, A photovoltaic technology review: History, fundamentals and applications Energies, vol. 15, n.º 5, p. 1823, March, 2022.

[2] A. Khatibi, F. R. Astaraei and M. H. Ahmadi, Generation and Combina- tion of the Solar Cells: A Current Model Review, Energy Sci. Eng., vol. 7, n.º 2, pp. 305–322, fevereiro, 2019.

[3] T. Burton, N. Jenkins, D. Sharpe and E. Bossanyi, Wind Energy Hand- book, 2ª ed. Hoboken, NJ: Wiley-Blackwell, março, 2011

[4] P. Andru e A. Botchkarev, The Use of Return on Investment (ROI) in the Performance Measurement and Evaluation of Information Systems, janeiro, 2011

[5] Discounted Payback for Measuring Simple, https://www.govinfo.gov/content/pkg/GOVPUB- C13- b8d7384734abd5754ef331828ed3974b/pdf/GOVPUB-C13-b8d7384734abd5754ef331828ed39 74b.pdf, Acedido: 26 de junho de 2024.

[6] Datasheet of SZ-100-33MF, https://cdn.enfsolar.com/z/pp/4l13tku587i0o /bea9d45b752ef1fe14ad60b9a5d6f01f2.pdf, Acedido: 22 de março de 2024.

[7] Datasheet of Aeolos-V 10kW, https://abei.ch/wp- content/uploads/2023/02/Aeolos-V 10kW-Brochure-1.pdf, Acedido: 22 de julho de 2024.

[8] Report on the techno-economic study, https://www.km3net.org/wp- content/uploads/2021/07/D10.3-KM3NeT-techno-economic-study.pdf, Acedido: 13 de junho de 2024.

[9] M. Edésio, E. Elias Lopes, D. Ruth e R. Nogueira, Proposta Metodológica para Validação de Imagens de Alta Resolução do Google Earth para a Produção de Mapas, janeiro, 2011.

[10] M. Engels, P. Boyd, T. Koehler et al., Smart and Green Energy (SAGE) for Base Camps Final Report, rel. téc., fevereiro, 2014.

[11] SIDC ruoqiang 100MW tower + 900MW PV CSP Project, https://solarpaces.nrel.gov/project/sidc-ruoqiang-100mw-tower-900mw- pv, Acedido: 29 de julho de 2024.


Résultats - RCA

Anti-Jamming para UAVs através de Inteligência Artificial baseada em Comportamento de Enxame

Alferes-Aluno Tm Tiago Silva

TPO Transmissões

Resumo - A utilização de Unmanned Aerial Vehicles (UAV) expandiu-se significativamente nos sectores civil e militar para a realização de tarefas estratégicas. Em comparação com as abordagens tradicionais, esta investigação explora a eficácia das técnicas *Anti-Jamming* para UAVs, tirando partido da Inteligência Artificial (IA) baseada no comportamento de enxame.

O estudo estabelece uma base teórica abrangente para a compreensão da investigação proposta, fornecendo uma análise aprofundada dos avanços atuais da *Electronic Warfare* (EW). Além disso, identifica ferramentas essenciais para a investigação, tais como modelos de antenas realistas e metodologias avançadas de IA.

Através de testes experimentais e simulações, este trabalho valida as hipóteses formuladas, resultando em provas concretas da eficácia das estratégias. As conclusões indicam que os algoritmos genéticos produzem bons resultados, embora incorram em tempos de simulação elevados. Em comparação, a abordagem *Reinforcement Learning* (RL) demonstra resultados promissores quando pré-treinada com dados realistas, alcançando eficiência dentro de restrições práticas de tempo.

Introdução

Os UAV são cada vez mais utilizados em operações civis e militares devido à sua versatilidade e capacidades autónomas. Em contextos militares, os UAV são particularmente valiosos para reconhecimento, combate e apoio logístico, proporcionando uma vantagem na recolha de informações e resposta rápida [1],[2]. No entanto, as comunicações dos UAV são altamente vulneráveis, o que pode reduzir significativamente a sua eficácia no campo de batalha. Tal como o salto de frequência, as medidas anti-*jamming* existentes têm muitas vezes de se adaptar a ambientes de dados dinâmicos e de alta velocidade, particularmente em enxames de UAV, onde as respostas coordenadas são essenciais.

Esta investigação aborda o desafio de manter a comunicação dentro de um enxame de UAVs em condições de interferência. A questão principal a que esta investigação procura responder é:

Pode um enxame de UAVs, atuando em formação coordenada, adotar medidas *anti-jamming* eficazes, otimizando conjuntamente parâmetros de comunicação como a formação e a configuração da antena, sem comprometer a missão?

Ferramentas de Desenvolvimento e de Simulação

A. OpenAI Gym

Permite a comparação direta de diferentes algoritmos num ambiente consistente, trata tarefas de simulação críticas, como o cálculo das distâncias dos nós e dos ângulos das antenas, a implementação de diagramas de radiação para antenas direcionais, a determinação do ganho da antena, o cálculo da potência de receção e interferência e a avaliação da capacidade de comunicação entre nós.

B. State Baseline3

É uma biblioteca que oferece implementações fiáveis de algoritmos RL em *PyTorch*. A sua integração com o *OpenAI Gym* permite comparações diretas entre algoritmos, e a sua estrutura personalizável permite a adaptação a necessidades específicas de investigação.

C. Seaborn

Uma biblioteca de visualização de dados *Python*, fornece uma interface de alto nível para explorar conjuntos de dados complexos. Esta biblioteca permite a visualização, interpretação e comparação eficazes dos resultados obtidos na investiga.

Metodologia

A. Modelo do Sistema

O modelo proposto explora as propriedades direcionais da antena de cada UAV para estabelecer ligações com menor suscetibilidade a interferências, bem como a determinação de posições estratégicas que favoreçam essas ligações.

Foram atribuídas capacidades direcionais a cada UAV para modelar o sistema de forma realista, exigindo um diagrama de radiação detalhado para calcular com precisão os ganhos de transmissão e receção entre os UAVs e o *jammer*. Com base na investigação [3] este estudo adaptou os valores de ganho típicos destas antenas para criar um modelo de radiação efetivo representado na Figura 1.

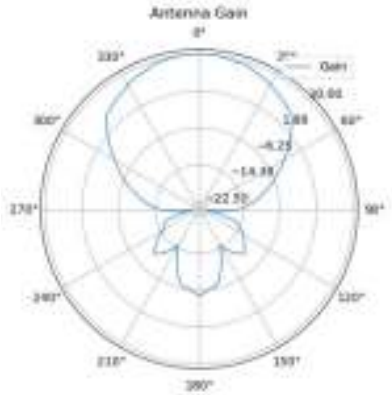


Figura 1: Diagrama de radiação da antena direcional

O ambiente de simulação modela e otimiza as comunicações do enxame de UAVs num espaço 2D, onde a otimização se centra na maximização das capacidades de ligação sob interferência do *jammer*, com direções de antena ajustáveis em 360 graus. Os UAVs partilham continuamente dados de posição e direcionais através de sensores ou protocolos de comunicação, permitindo o cálculo das potências de transmissão, receção e interferência com base nos ângulos e distâncias de transmissão/receção.

B. Formulação do Problema

O estudo utiliza um ambiente de simulação bidimensional em que a posição de cada UAV é definida em coordenadas cartesianas (x,y) e a direção da sua antena é representada como um ângulo entre 0° e 360°. A capacidade de comunicação entre UAVs é influenciada pela distância entre nós, pela potência de transmissão, pela orientação da antena e pela interferência de *jammers*. A Função Objetivo para este problema de otimização é definida na Equação (1), maximizando o produto ponderado da capacidade média C_(média)e da capacidade mínima C_mínima, com pesos α e β que permitem a priorização relativa de cada termo. Esta aproximação não linear garante uma decisão equilibrada com base nas necessidades específicas da aplicação.

$$f_{objetivo}(p,\theta) = C_{média}(p,\theta)^{\alpha} \cdot C_{mínima}(p,\theta)^{\beta} \quad (1)$$

A Tabela 1 especifica todas as variáveis adaptáveis neste sistema de comunicações.

Símbolo	Descrição	Unidade
B	Largura de Banda para a comunicação	Hz
P_{Jammer}	Potência de transmissão do jammer	dBm
P_{txUAV}	Potência de Transmissão de cada UAV	dBm
N_{UAV}	Número de UAVs do sistema	
L	Comprimento da área de interesse	metros
W	Largura da área de interesse	metros
S	Distância entre pontos discretos	metros
R	Diagrama de radiação das antenas	
γ	Expoente de perda	
d_0	Distância de referência	metros
T	Tempo limite da simulação	segundos

Tabela 1: Variáveis Adaptáveis para o Sistema de Comunicações

C. Abordagem Algoritmo Genético

Dada a complexidade do ambiente em estudo, a exploração de um espaço de ação pode tornar-se computacionalmente exigente. Para uma melhor compreensão, é necessário clarificar o conceito de cromossoma neste contexto. No contexto específico dos UAVs, um cromossoma é uma sequência de valores (genes) que codificam as direções das antenas (e posteriormente as posições) para cada UAV. Nesta investigação, cada cromossoma é constituído por um número de genes igual ao número de UAVs do sistema. Cada gene codifica uma direção adquirida pelo UAV. A Figura 2 serve de exemplo.

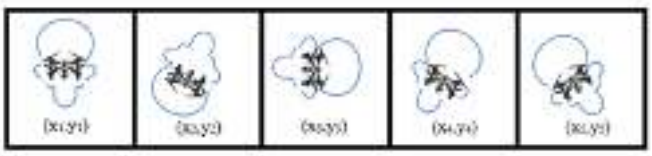


Figura 2: Composição de um cromossoma

Para otimizar as comunicações dos UAVs, o AG começa por inicializar uma população de cromossomas aleatórios, cada um codificando as posições dos UAV e as direções das antenas. A aptidão de cada cromossoma corresponde à função objetivo e é calculada com base nas posições e direções do UAV no ambiente. Através de um processo de seleção que envolve a seleção de torneios (em que o melhor cromossoma de cada grupo avança), o algoritmo incentiva topologias favoráveis.

O processo foi dividido em duas fases: Otimização da posição e otimização da direção da antena. Primeiro, a disposição espacial ideal dos UAVs é determinada para melhorar a conetividade da rede, a capacidade de comunicação e a minimização de interferências. Uma vez fixadas as posições, a segunda fase ajusta os ângulos das antenas dos UAVs para maximizar o ganho de sinal e minimizar a interferência. Esta abordagem em duas fases reduz a complexidade da pesquisa AG, aumentando assim a eficiência da convergência e melhorando a qualidade da solução final.

D. Abordagem *Reinforcement Learning*

A formulação MDP estrutura o ambiente do enxame de UAVs para o agente interagir com estados, ações e transições. Cada estado consiste em posições de UAVs, direções de antena, posições de jammer e uma matriz de capacidades que representam as condições ambientais atuais. As ações incluem movimentos x/y e ajustes da antena, formando um vetor de ação completo. A função de transição de estado atualiza as posições e as direções das antenas e recalcula as capacidades de comunicação com base na distância do UAV, nos ângulos das antenas e nas variáveis de potência. Finalmente, a função de recompensa reflete a função objetivo, incentivando a maximização das capacidades de comunicação globais e mínimas, assegurando a conetividade e evitando a fragmentação da rede.

O objetivo do MDP é encontrar uma política ótima π que maximize o valor esperado das recompensas acumuladas ao longo do tempo. O agente aprende a ajustar as posições e direções das antenas dos UAVs de forma ótima para maximizar o desempenho da rede de comunicações. A interação agente-ambiente pode ser descrita pela Figura 3.

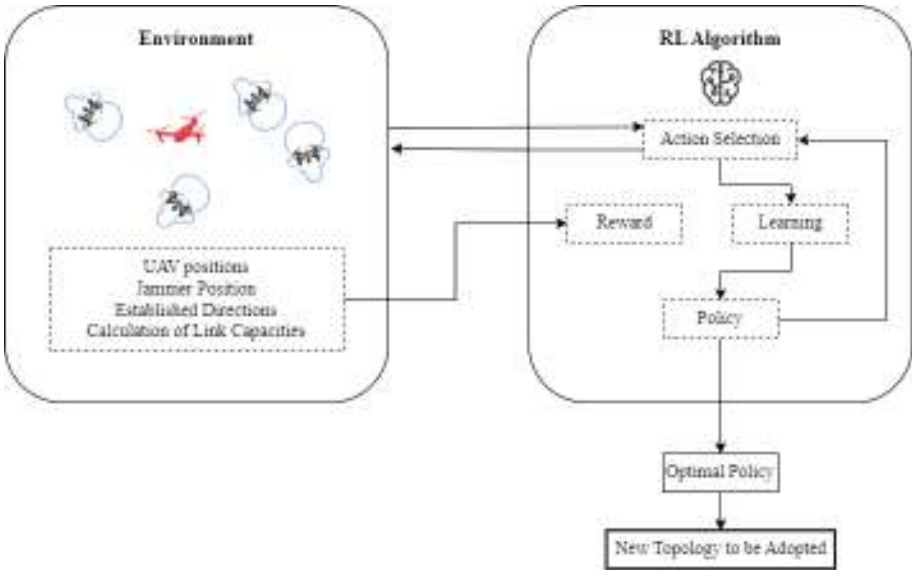


Figura 3: Interação Agente-Ambiente, adaptado de [4]

Cenários

A criação de cenários realistas de complexidade variável permite explorar o comportamento e verificar o desempenho em diferentes níveis de procura.

A. Cenário Estático com Exploração da Direcionalidade da Antena

Num cenário de enxame de UAV estático, o foco está na avaliação da direção da antena dos UAVs para estabelecer ligações de comunicação sem interferências, evitando as perturbações do agente malicioso. Os principais fatores de avaliação incluem a eficácia do alinhamento da antena para as transmissões necessárias, a eficiência da transmissão e receção do sinal num ambiente fixo e a capacidade do enxame para mitigar a interferência e otimizar a utilização do espetro.

B. Cenário Estático com Exploração da Direcionalidade das Antenas e Posições dos UAVs

Neste cenário, o posicionamento espacial do enxame de UAVs e a direcionalidade da antena são considerados, permitindo que os UAVs individuais ajustem as suas posições. Operando dentro de uma área discretizada em diversas posições, o desempenho do enxame é avaliado com base na coordenação para otimizar a topologia, o impacto dos ajustes da topologia na comunicação, conetividade e alcance num ambiente dinâmico, e a resiliência a alterações na topologia da rede.

C. Cenário com um enxame em progressão

Neste cenário dinâmico, o enxame de UAVs desloca-se continuamente no espaço, exigindo uma adaptação constante da direcionalidade da antena para manter a conetividade à medida que a área operacional se desloca juntamente com o enxame. A avaliação inclui os fatores mencionados anteriormente, centrando-se na adaptabilidade da rota e na manutenção da conetividade num ambiente móvel e dinâmico.

Simulação

A. Parametrização

Como propõe esta investigação, a análise da utilização do RL em cenários realistas exige uma parametrização realista. Os parâmetros aplicados são detalhados na Tabela 2.

Parameter	Valor
Número de UAVs	4
Largura de banda	$2.4e^9 Hz$
Potência de transmissão do UAV	20 dBm
Distância de referência d_0	1 m
Valor de perda à distância de referência	30 dB
Potência do jammer	100 dBm
Expoente de perda γ	2
Tamanho da área de interesse	50m x 40m
Distância entre pontos discretos da área de interesse	5 m

Tabela 2: Parâmetros aplicados ao enxame de UAVs

B. AG

Os seguintes parâmetros do AG foram analisados: *population size, generations, mutation rate* e *crossover rate*. Os parâmetros finais foram selecionados com base nos resultados obtidos pelas várias combinações testadas.

C. PPO

Neste estudo, o algoritmo PPO verificou a necessidade de ser aplicado um pré-treino com um conjunto de dados. A estrutura do conjunto de dados introduzido pode ser vista na Tabela 3.

Posição do Jammer	Direções	Recompensa
[76.3, 15.7]	[210.6, 257.3, 167.1]	18851.4
[89.3, 48.0]	[43.4, 211.8, 186.7]	347672.2
...	...	...

Tabela 3: Formato do Data Set de treino

D. SAC

O valor da recompensa foi normalizado para atenuar a frequência de *outliers* e obter um treino mais estável. Esta necessidade decorre da vasta gama de valores que a recompensa pode assumir. Com o ajuste correto dos hiperparâmetros da Tabela 4.

Hiperparâmetro	Valor	Descrição
Actor L. Rate	1e-1	Taxa de aprendizagem para a rede Actor.
Critic L. Rate	1e-1	Taxa de aprendizagem para as redes *Critic 1* e *Critic 2*.
Gamma (γ)	0.99	Fator de desconto de futuras recompensas.
Tau (τ)	0.001	Taxa de atualização das redes *Critic 1* e *Critic 2*.
Alpha (α)	0.01	Coeficiente de entropia que controla o grau de exploração.
Buffer Size	10,000	Capacidade máxima do *buffer*.
Batch Size	1024	Número de amostras utilizadas para cada atualização de gradiente.

Tabela 4: Hiperparâmetros usados no algoritmo SAC

Resultados

Os resultados obtidos através das simulações fornecem comparações perspicazes entre os três cenários de estudo, cada um com complexidade progressivamente crescente, que mostram os pontos fortes e as limitações das abordagens GA e RL.

A. Cenário 1: Estático com Exploração da Direcionalidade das Antenas

Para o primeiro cenário, ambas as abordagens obtiveram resultados idênticos. Isto significa que ambos os algoritmos podem efetivamente demonstrar versatilidade e adaptabilidade quando confrontados com vários contextos ou cenários.

B. Cenário 2: Estático com Exploração da Direcionalidade das Antenas e Posições dos UAVs

O AG conseguiu adquirir posições favoráveis para as comunicações e otimizou a direcionalidade das antenas. Verificou-se uma rápida convergência na determinação das posições dos UAVs relativamente às direções das antenas, com um valor da FO significativamente mais elevado quando se aplicam antenas direcionais em comparação com antenas omnidirecionais. Apesar do desempenho satisfatório na redução da interferência do *jammer* e na aproximação dos UAVs, o AG requer um longo tempo de simulação para obter configurações ótimas, limitando a sua viabilidade para cenários operacionais dinâmicos.

Com um conjunto de dados externos, o PPO foi testado para otimizar as posições cartesianas dos UAVs e as direções das antenas. A análise mostrou que, embora o PPO posicione eficazmente os UAVs longe do bloqueador e perto uns dos outros, teve dificuldades em convergir para direções de antena adequadas para otimizar as comunicações. O algoritmo mostrou instabilidade na recompensa média durante o treino, indicando que o PPO tende a convergir para soluções sub-ótimas devido à exploração limitada do espaço de soluções.

O SAC revelou-se o algoritmo mais eficaz, alcançando um aumento rápido e estável da recompensa média durante o treino. Com ajustes nos hiperparâmetros, o SAC pode posicionar os UAVs longe do *jammer* e ajustar as direções das antenas de forma eficiente para maximizar a capacidade de comunicação. O SAC obteve melhores resultados do que o PPO ao criar uma topologia que favorece o desempenho da rede com base na exploração otimizada do ambiente, permitindo ajustes mínimos à política final para manter uma recompensa elevada.

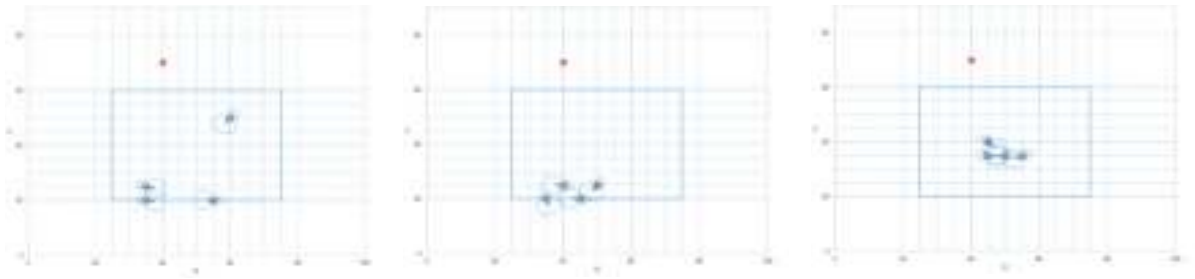


Figura 5 Resultado obtido através do algoritmo AG, PPO e SAC

C. Cenário 3: Enxame em Progressão

Neste cenário, foi realizado um estudo comparativo entre o AG e o algoritmo SAC para otimizar a progressão e a formação de enxames de UAVs. Devido a uma restrição de 7,5 segundos para atualizações de topologia, o AG foi cuidadosamente parametrizado, usando uma população de 14 cromossomos em 40 gerações, para produzir resultados dentro de um tempo médio de simulação de 6,43 segundos.

Os resultados iniciais mostram que, apesar do tempo de processamento limitado, o AG pode agrupar eficazmente os UAVs e direcionar as antenas para reduzir a interferência. No entanto, é possível obter melhorias com um tempo de simulação alargado, permitindo que o AG explore uma gama mais ampla de posições e orientações.

Avaliámos o desempenho do algoritmo SAC neste cenário com base no treino prévio e na otimização de parâmetros realizados em cenários anteriores. Ao observar as configurações ao longo do tempo (por exemplo, de 7,5s a 45,0s), fica evidente que o algoritmo SAC permite uma aquisição de posições e um alinhamento direcional mais eficazes do que as abordagens anteriores.

Notavelmente, o SAC alcança um agrupamento mais denso de UAVs dentro do enxame, e os alinhamentos direcionais apresentam menos dispersão. Ao explorar mais eficazmente as profundidades subótimas, o SAC promove uma configuração mais coesa do enxame, com menor variância direcional, aumentando a sua resiliência contra *jamming* e interferências. A Figura 6 mostra os resultados obtidos.

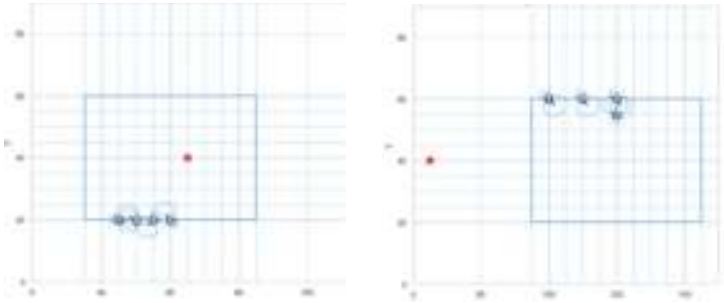


Figura 6: Resultado do algoritmo SAC para 7.5 e 37.5 s

Conclusões

Este estudo avaliou três cenários para comparar o desempenho de algoritmos genéticos e métodos de RL (PPO e SAC) em medidas *anti-jamming* em enxames de UAVs.

No primeiro cenário, com posições estáticas dos UAVs e ajustes apenas nas direções das antenas, o AG apresentou soluções comparáveis ao PPO e SAC, destacando a importância de um treino adequado do RL. No segundo cenário, com a inclusão do movimento dos UAVs, o desempenho do AG foi dependente do tempo de simulação disponível, enquanto o RL, especialmente o SAC, demonstrou maior eficácia devido a atualizações dinâmicas da política pela interação com o ambiente. No terceiro cenário, com o movimento progressivo do enxame ao longo do tempo, o RL superou significativamente o AG, mostrando melhor mitigação de interferências sob restrições de tempo.

De forma geral, o AG obteve resultados eficientes, dependendo diretamente do tempo de simulação. Por outro lado, embora o RL exija um pré-treino mais complexo e demorado, oferece resultados mais rápidos e precisos, pois o modelo pode ser pré-treinado para cenários futuros. Assim, o RL é uma ferramenta promissora e eficaz para obter topologias otimizadas contra interferências maliciosas em cenários dinâmicos, enquanto o AG é inviável em tempo real, onde topologias sólidas devem ser determinadas no menor tempo possível.

Bibliografia

[1] J. Kim, C. Park, J. Ahn, Y. Ko, J. Park, and J. C. Gallagher, "Realtime uav sound detection and analysis system," in 2017 IEEE Sensors Applications Symposium (SAS). IEEE, 2017, pp. 1–5.

[2] M. R. Brust and B. M. Strimbu, "A networked swarm model for uav deployment in the assessment of forest environments," in 2015 IEEE Tenth international conference on intelligent sensors, sensor networks and information processing (ISSNIP). IEEE, 2015, pp. 1–6.

[3] C. U. Lee, G. Noh, B. Ahn, J.-W. Yu, and H. L. Lee, "Tilted-beam switched array antenna for uav mounted radar applications with 360° coverage," Electronics, vol. 8, no. 11, p. 1240, 2019.

[4] R. Amiri, H. Mehrpouyan, L. Fridman, R. K. Mallik, A. Nallanathan, and D. Matolak, "A machine learning approach for power allocation in hetnets considering qos," in 2018 IEEE international conference on communications (ICC). IEEE, 2018, pp. 1–7.

Estratégias de *Jamming* e *Spoofing* para Aplicações Anti-Drones

Alferes-Aluno Tm Younes Zidane
TPO Transmissões

Resumo - Este artigo investiga o desenvolvimento e a avaliação de técnicas de empastelamento (*jamming*) e de falsificação de sinais (*spoofing*) para perturbar os sistemas de comunicação e de navegação de Veículos Aéreos Não Tripulados (VANTs) em zonas restritas. Utilizando a tecnologia de *Software Defined Radio* (SDR), foi desenvolvido um sistema adaptável para neutralizar os drones, perturbando os seus sinais de controlo e serviços de geolocalização. Testes experimentais em drones comerciais demonstraram a eficácia do empastelamento por radiofrequência (RF) na interrupção do controlo e da transmissão de imagens, enquanto o *spoofing* emitiu com sucesso sinais falsos do *Global Navigation Satellite System* (GNSS) e interferiu com o comportamento dos drones.

Introdução

Os VANTs desenvolveram-se rapidamente e são atualmente utilizados em sectores como da fotografia, cartografia e entregas [1]. As preocupações com a segurança, especialmente devido a conflitos recentes, alimentaram o interesse em tecnologias contra drones [1]. Estes sistemas, que detetam drones utilizando sinais de rádio e radar, têm como objetivo evitar acidentes e ameaças como o terrorismo. No entanto, a integração de sistemas de combate a drones em ambientes críticos apresenta desafios, incluindo questões regulamentares, técnicas e de custos [2].

Contextualização

A. Normas de Comunicação para os VANTs

O sistema de comunicação de um VANT inclui quatro ligações principais: Navegação, Rádio Controlo (RC), Telemetria e Vídeo. A ligação de navegação utiliza um recetor GNSS para fornecer dados de posição e velocidade, enquanto a ligação RC transmite comandos do operador com baixa latência. A telemetria envia informações sobre o estado do drone, e a ligação de vídeo transmite imagens da câmara ao controlador [3]. O Wi-Fi, amplamente utilizado, é uma tecnologia proeminente para comunicação entre a estação terrestre e o drone, operando nas bandas de 2,4 GHz (2400–2500 MHz) e 5 GHz (5725–5925 MHz), conforme as normas IEEE 802.11 [4,5].

1) Modulação e Protocolos dos VANTs: As ligações RC, telemetria e de vídeo usam canais RF, como o Wi-Fi, sendo a transmissão de vídeo predominantemente baseada em *Orthogonal Frequency-Division Multiplexing* (OFDM) [3,6]. Técnicas de modulação como *Frequency-Hopping Spread Spectrum* (FHSS), *Direct Sequence Spread Spectrum* (DSSS) e OFDM são comuns em drones. A telemetria na banda de 2,4 GHz usa OFDM e DSSS, enquanto na banda de 5 GHz é dominada por OFDM [6,7].

2) Fundamentos do GNSS: Os sistemas GNSS, como GPS, GLONASS, Galileo e BeiDou [8], operam na banda L, permitindo a navegação por meio do cálculo do tempo de viagem do sinal e da posição do satélite. Esses sinais incluem uma portadora em frequência RF e códigos de ruído pseudo-aleatório, como os códigos C/A e P do GPS. Essenciais para drones comerciais, suportam funções como *return-to-home* em caso de perda de sinal. Na UE, GPS e Galileo operam de forma interoperável, com o GPS utilizando as bandas L1 (1575,42 MHz), L2 (1227,60 MHz) e L5 (1176,45 MHz) [9].

B. *Spoofing* de Radiofrequências

O *spoofing* envolve o envio de comunicações fraudulentas que aparentam vir de uma fonte confiável, com o objetivo de enganar o destinatário. No caso de sinais GPS, é possível induzir recetores a aceitar dados de localização falsificados, comprometendo a integridade da informação baseada na localização [10]. As *No Fly Zones* (NFZ), áreas onde o voo de determinadas aeronaves é proibido, são estabelecidas por entidades militares ou governamentais para mitigar ameaças, especialmente em áreas de conflito ou eventos de grande visibilidade. A violação dessas zonas por *spoofing* pode levar à aterragem automática ou impedir a decolagem de drones afetados [11].

C. *Jamming* de Radiofrequências

O empastelamento de RF interrompe a comunicação entre um drone e o operador, afetando a sua capacidade de receber instruções. Os sinais GNSS são particularmente vulneráveis devido à sua fraqueza, e os bloqueadores de GPS podem impedir as funções de *return-to-home*, conduzindo a avarias ou colisões. As principais técnicas de interferência de RF incluem [3,7]:

• *Barrage Jamming*: O ruído de banda larga reduz o rácio sinal-ruído (SNR), aumentando as taxas de erro e diminuindo a capacidade do canal.

• *Sweep Jamming*: Um sinal de banda estreita varre as frequências, simulando os efeitos de interferência de barragem em altas taxas de varredura.

• *Follower Jamming*: Acompanha as alterações de frequência nos sistemas FHSS para bloquear as frequências recentemente selecionadas.

Conceção do Sistema e Metodologia

A. *Hardware* e *Software*

O sistema inclui um computador portátil, o ADALM-PLUTO para modulação e transmissão (32 MHz a 3,8 GHz, -4 dBm a 0 dBm), um amplificador WYDZ-PA-1G-3GHz-1W (30 dB de ganho, 1 W), e antenas otimizadas: YAGI WIFI para 2,4 GHz e outra de 1,5 GHz. Os drones testados operam em 2,4 GHz e 5,8 GHz, com o Autel Evo Nano+ usando também 5,150-5,250 GHz e o Husban Zino Mini Pro com backup 4G. O *software* usado incluiu GNU Radio (3.10.1.1) no Ubuntu 24.04.1 LTS e *Visual Studio Code* para ajustar *scripts Python*.

B. Metodologia

1) *Barrage Jamming* do GNSS: O GNU Radio foi usado para desenvolver *scripts* de interferência em sinais GNSS, com destaque para o *barrage jamming* (Figura 1). Essa técnica envolve a transmissão contínua de ruído de alta potência no espectro GNSS. O aumento do nível de ruído compromete a receção dos sinais legítimos, causando perda de precisão ou funcionalidade posicional nos recetores GNSS dos drones.

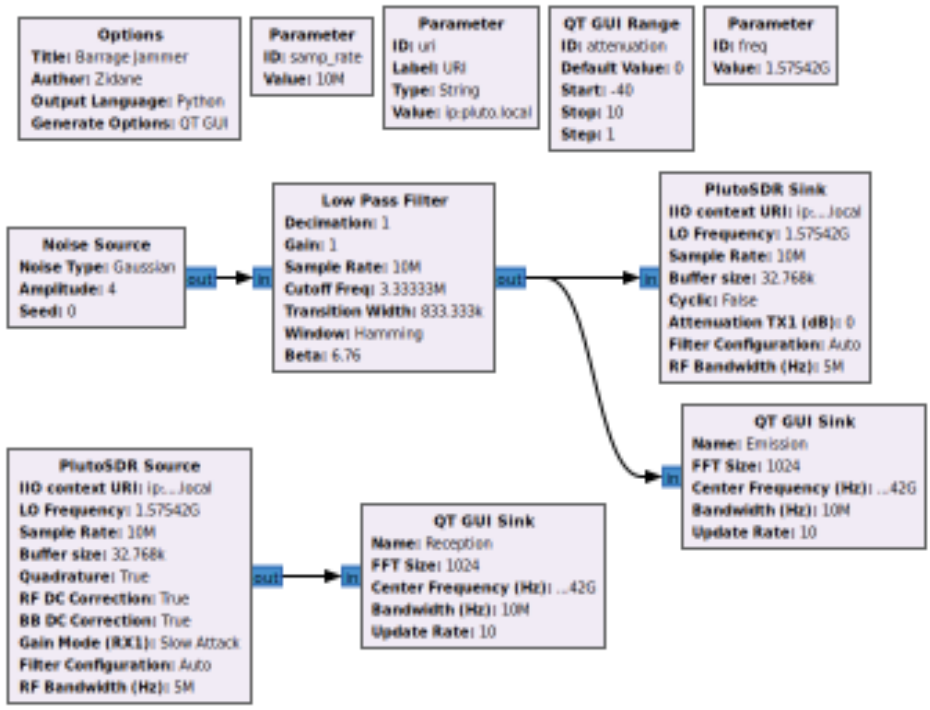


Figura 1: Script utilizado para implementar *Barrage jamming* no GNSS

O *script* utiliza uma taxa de amostragem de 10 MHz e gera ruído gaussiano. Um filtro passa-baixo limita a largura de banda a 3,333 MHz, focando na banda GPS L1, com frequência de corte correspondente a um terço da taxa de amostragem. O bloco *PlutoSDR Source* captura sinais na frequência GPS L1, enquanto o *PlutoSDR Sink* transmite o ruído filtrado na mesma frequência e taxa de amostragem.

2) BPSK *Jamming* do GNSS: A interferência com conhecimento de protocolos imita e sobrepõe o sinal original, otimizando a relação potência-largura de banda. Em sistemas GPS, que usam modulação BPSK, esta técnica gera um sinal interferente que replica a modulação, levando o recetor a interpretar o sinal interferente como legítimo. A Figura 2 apresenta o script GNU Radio desenvolvido para esta implementação.

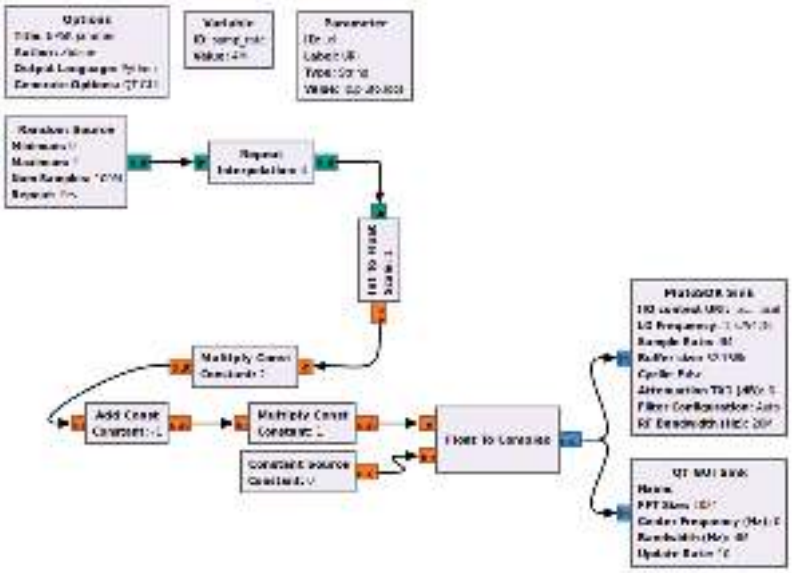


Figura 2: *Script* utilizado para implementar BPSK *jamming* no GNSS

O *script* gera uma sequência de bits aleatórios à taxa de 1,023 Mbit/s, correspondente à taxa de chip do GPS, com período de amostragem de 100 M. Um fator de interpolação de 4 ajusta a taxa de amostragem para 4,092 MHz, garantindo compatibilidade com o PlutoSDR Sink. Os bits são então mapeados para uma constelação BPSK representando +1 e -1. O PlutoSDR Sink transmite o sinal BPSK modulado na frequência central GPS L1, com buffer de 32,768 ks, transmissão não cíclica e atenuação TX1 ajustada para 0 dB.

3) *Spoofing* do GNSS: Um ataque de *spoofing* foi realizado utilizando o simulador GPS-SDR-SIM, com o objetivo de manipular a posição de um recetor alvo. Este simulador gera sinais realistas que, ao serem convertidos em RF pelo SDR, tornam-se adequados para experimentos de *spoofing*. O GPS-SDR-SIM permite configurar trajetórias específicas através de ficheiros. Nesta investigação, sinais GPS simulados foram transmitidos pelo SDR com uma taxa de amostragem de movimento de 10 Hz, garantindo precisão na simulação de movimentos.

4) *Barrage jamming* de RC e Vídeo: O *script* implementado no Barrage *jamming* do GNSS foi ajustado para interferir em sinais RC e de vídeo na banda de 2,4 GHz. A largura de banda foi configurada para 20 MHz, largura de banda máxima do SDR, com amplitude do ruído definida em 2, garantindo interferência forte sem saturar o dispositivo. No entanto, estes parâmetros não cobrem toda a banda de 2,4 GHz (80 MHz), o que levou à necessidade de modificações no código *Python* gerado pelo GNU Radio para estender a cobertura a toda a banda. A frequência de iio_pluto_sink_0 foi ajustada para utilizar este parâmetro. As variáveis *start_frequency* (2,405 GHz) e *stop_frequency* (2,475 GHz) foram definidas. A função *update_frequency* foi configurada para atualizar a frequência a cada 5 segundos. Drones que operam na banda de 2,4 GHz frequentemente utilizam a tecnologia FHSS, que altera aleatoriamente as frequências de operação. Para interromper essa comunicação, foi desenvolvida uma nova estratégia de *jamming*. Na função *main*, foi definida uma lista de frequências centrais, incluindo [2,41 GHz, 2,425 GHz, 2,44 GHz, 2,455 GHz, 2,47 GHz]. A função *update_frequency* foi modificada para usar o módulo *random*, permitindo que, em vez de incrementar as frequências sequencialmente, ela selecione aleatoriamente uma frequência da lista predefinida.

Resultados e Discussão

A. *Jamming* e *Spoofing* do GNSS

Os testes práticos desta implementação foram realizados no Campo Militar de Santa Margarida, durante o exercício ARTEX24. Durante os testes, a posição tanto do operador quanto do *jammer* foi mantida fixa. Para avaliar as implementações, foi utilizado um Analisador de *Sinal/Espectro Rohde \& Schwarz FSV30*. Além disso, a potência de saída no terminal do amplificador foi medida para estimar a eficácia potencial do ataque, empregando um atenuador de 30 dB para proteger o equipamento durante as medições.

1) *Barrage Jamming* do GNSS: A Figura 3 apresenta o espectro do sinal com a frequência de corte definida como um terço da taxa de amostragem (SR/3).

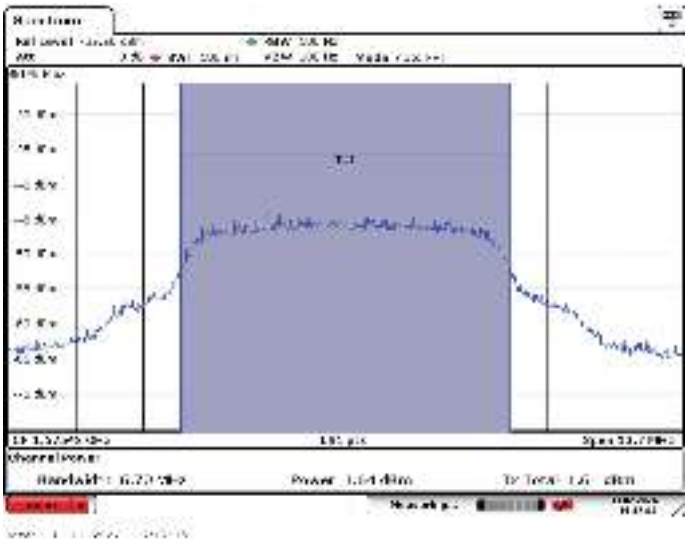


Figura 3: Espectro do sinal de *Barrage Jamming* de GNSS (fc=SR/3)

Considerando a atenuação de 30 dB, somada à potência obtida de 1,64 dBm, obtemos 31,6 dBm, com uma Potência Isotrópica Radiada Eficaz (EIRP) de 43,6 dBm quando conectada a uma antena Yagi de 12 dBi.

Os resultados de interferência apresentados na Tabela 1 foram promissores. A distância (D) entre o *jammer* e o drone foi variada, com o jammer fixo enquanto o drone se movia para avaliar a eficácia do jamming. O sinal verde de *checkmark* indica sucesso total no *jamming*, resultando em uma interrupção de 100% na receção do sinal de geolocalização, tornando o drone incapaz de receber qualquer informação de satélite. O "X" a vermelho representa uma tentativa de *jamming* falhada, onde a receção do sinal de geolocalização não foi completamente interrompida.

Drone/Distância (D)	80 m	100 m	120 m	130 m	140 m
DJI Mini 3	✓	✓	✓	✗	✗
DJI Mini 3 Pro	✓	✓	✓	✗	✗
Autel Evo Nano+	✓	✓	✓	✓	✗
Husban Zino Mini Pro	✓	✓	✓	✓	✓
ZLL SG 108	✓	✓	✓	✓	✓

TABELA 1- Efetividade do *Barrage jamming* de GNSS a diferentes distâncias entre o jammer e o drone

A eficácia do *jamming* foi avaliada verificando se o drone conseguia se conectar aos satélites apesar da interferência. A principal consequência do *jamming* do GNSS foi a falha na função *return-to-home*. Sem essa função, o drone perde a capacidade de determinar sua localização e pode se perder, especialmente quando controlado à distância e sem contato visual. Diferentes modelos de drones reagiram de maneira distinta ao *jamming*: os modelos DJI e Husban perderam a conexão com os satélites, mas permaneceram no estado comandado pelo último sinal recebido. Já os modelos Autel e ZLL responderam de forma mais segura, realizando imediatamente um procedimento de aterragem, mitigando riscos associados ao *jamming*.

2) BPSK *Jamming* do GNSS: O espectro do sinal transmitido para a implementação do BPSK *jamming* está ilustrado na Figura 4.

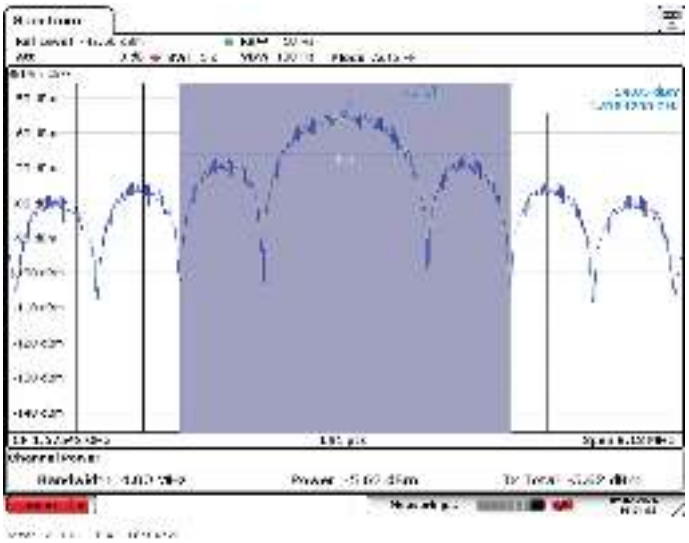


Figura 4: Espetro do sinal de BPSK *jamming* no GNSS

A potência de saída medida foi de -5,6 dBm. Considerando o ganho do amplificador (30 dB) e o ganho da antena (12 dBi), o EIRP total calculado foi de aproximadamente 36,4 dBm. A Tabela 2 apresenta os resultados da eficácia do *jamming*, com a distância (D) representando a separação entre o *jammer* e o drone.

Drone/Distância (D)	80 m	100 m	120 m	130 m	140 m
DJI Mini 3	✓	✓	✓	✓	✗
DJI Mini 3 Pro	✓	✓	✓	✓	✗
Autel Evo Nano+	✓	✓	✓	✓	✗
Husban Zino Mini Pro	✓	✓	✓	✓	✓
ZLL SG 108	✓	✓	✓	✓	✓

TABELA 2 - Efetividade do BPSK *jamming* de GNSS a diferentes distâncias entre o *jamming* e o drone

A modulação BPSK demonstra maior eficiência do que o *barrage jamming* para GNSS, especialmente em distâncias maiores e com menor potência, devido a dois fatores principais: a densidade de potência dos sinais BPSK concentra energia em uma faixa de frequência estreita, alinhada com as utilizadas pelos sistemas GNSS, e a semelhança de modulação com os sinais GNSS, o que dificulta a distinção entre sinais legítimos e sinais de *jamming* pelos recetores.

3) *Spoofing* do GNSS: Foi simulado um ataque de *spoofing* com SDR transmitindo dados geoespaciais falsos. O primeiro método foi o *spoofing* estático para uma posição aleatória (Tóquio, Japão), sem afetar o comportamento do drone. Em seguida, foi realizado *spoofing* estático para uma NFZ (Aeroporto Francisco Sá Carneiro, Porto, Portugal), impactando os drones DJI, que ativaram medidas de proteção, como avisos e contagem regressiva para o pouso automático.

O *spoofing* dinâmico com variação de altitude, utilizando um arquivo CSV com 3000 pontos, gerou comportamentos erráticos nos drones ZLL SG 108 e Autel Evo Nano+, enquanto os DJI mantiveram estabilidade. No *spoofing* dinâmico para uma NFZ com altitude zero, os drones tentaram pousar prematuramente, aumentando os riscos de colisão. O *jamming* combinado com sinais falsificados foi eficaz contra os drones DJI.

As respostas ao *spoofing* dinâmico variaram: os DJI Mini 3 e Mini 3 Pro mantiveram estabilidade no voo estacionário, mas perderam o controle em movimento, ativando o pouso automático. O Autel Evo Nano+ ficou instável, subindo descontroladamente antes de pousar de forma errática. O Husban Zino Mini Pro perdeu o controle em movimento, colidindo sem iniciar o pouso automático, e o ZLL SG 108 teve

B. *Barrage Jamming* de RC e Vídeo

A eficácia do *jamming* foi avaliada por meio de testes realizados em diferentes locais, como o Campo Militar de Santa Margarida e a Academia Militar de Amadora. Para garantir a precisão, a distância entre o operador e o drone foi significativamente maior que a distância entre o *jammer* e o drone, permitindo que o *jamming interferisse* efetivamente na comunicação. O *jammer* foi posicionado a 6 metros do drone, garantindo um sinal de *jamming* forte o suficiente para impactar o GNSS do VANT. A distância entre o operador e o drone (denotada como D) foi variada durante os testes para avaliar como o *jamming* afetava o controle do drone. A análise de espectro, ilustrada na Figura 5, mostra os padrões de emissão para as duas implementações de *barrage jamming*: uma varredura ampla da banda de 2,4 GHz e a mudança aleatória de frequências.

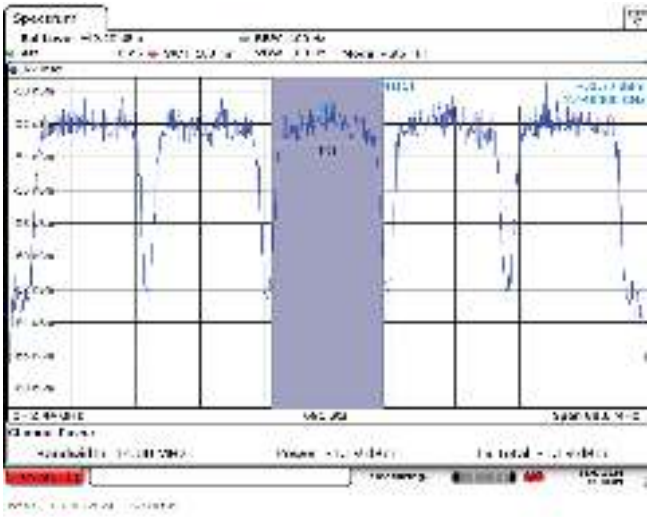


Figura 5: Espetro do sinal de *Barrage Jamming* na banda 2.4 GHZ

A série de cálculos foi realizada para estimar a intensidade do sinal na saída da antena do sistema. O sinal de saída inicial no amplificador foi medido em -1,2 dBm. Considerando a atenuação de 30 dB do atenuador e o ganho de 18 dBi da antena Yagi, a EIRP na saída da antena foi calculada em aproximadamente 46,8 dBm. A Tabela 3 reúne os resultados.

Drone/Distância (D)	30 m	50 m	80 m	100 m	120 m
DJI Mini 3	✗	✗	✗	✗	✓
DJI Mini 3 Pro	✗	✗	✗	✗	✓
Autel Evo Nano+	✗	✓	✓	✓	✓
Husban Zino Mini Pro	✗	✗	✗	✗	✗
ZLL SG 108	✓	✓	✓	✓	✓

TABELA 3- Efetividade do *Barrage jamming* de RC e vídeo a diferentes distâncias entre o operador e o drone.

A análise dos testes revelou desempenho semelhante entre os drones DJI, com operação estável até 40 metros, quando surgiram leves interferências. A partir de 85 metros, a conexão foi afetada, com falhas na transmissão de vídeo e atrasos nas manobras, culminando em perda total de conexão a 120 metros. O Autel Evo Nano+ mostrou maior vulnerabilidade, sendo neutralizado a partir de 50 metros. O Husban Zino Mini Pro foi imune ao *jamming* devido à possibilidade de alternar para comunicação 4G. Já o ZLL SG 108, sem interface visual, foi o mais afetado, tornando-se incontrolável a apenas 30 metros.

Conclusão

Este estudo focou no desenvolvimento de contramedidas de *jamming* para neutralizar os sistemas de comunicação de drones, com ênfase em proteger áreas sensíveis e infraestruturas. O sistema baseado em SDR mostrou-se eficaz, combinando *jamming* em barragem e técnicas como o *jamming* BPSK para interferência GNSS, adaptando-se aos desafios dos VANTs modernos.

Os testes realizados, tanto em ambientes controlados quanto em campo, demonstraram a eficácia do sistema. O *jamming* em barragem foi eficiente para interromper controle e transmissões de vídeo, embora o Husban Zino Mini Pro, com comunicação 4G, tenha revelado limitações. O *jamming* BPSK foi superior em precisão e alcance para interferir na navegação GNSS. O spoofing dinâmico, combinado com zonas de exclusão aérea e manipulação de altitude, provou ser eficaz para forçar pousos ou induzir comportamentos erráticos

Em resumo, a pesquisa apresenta uma solução adaptável e de baixo custo para *jamming* e *spoofing* de drones, fornecendo uma base sólida para proteger infraestruturas críticas contra atividades não autorizadas de VANTs.

Bibliografia

[1] D. Zmyslowski, P. Skokowski, and J. Kelner, "Anti-drone Sensors, Effectors, and Systems-A Concise Overview." TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, vol. 17, no. 2, p. 455–461, 2023.

[2] G. Abro, S. Zulkifli, R. Masood, V. Asirvadam, and A. Laouiti, "Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats," Drones, vol. 6, no. 10, p. 284, 2022.

[3] D. J. Rozenbeek, "Evaluation of Drone Neutralization Methods using Radio Jamming and Spoofing Techniques," Ph.D. dissertation, KTH Royal Institute of Technology, 2020. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-279557.

[4] M. A. Jasim, H. Shakhatreh, N. Siasi, A. H. Sawalmeh, A. Aldalbahi, and A. Al-Fuqaha, "A Survey on Spectrum Management for Unmanned Aerial Vehicles (UAVs)," IEEE Access, vol. 10, p. 11443–11499, 2022.

[5] S. I. Han, "Survey on UAV Deployment and Trajectory in Wireless Communication Networks: Applications and Challenges," Information, vol. 13, no. 8, p. 389, 2022.

[6] D. Torrieri, Direct-Sequence Systems. Springer International Publishing, 2021, p. 81–150.

[7] O. Simon and T. Gotthans, "A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception," Electronics, vol. 11, no. 19, p. 3025, 2022.

[8] EU Agency for the Space Programme, "What is GNSS," https://www.euspa.europa.eu/eu-space-programme/galileo/what-gnss, accessed: 2024-08-23.

[9] Navipedia, "GPS Signal Plan," https://gssc.esa.int/navipedia/index.php/ GPS Signal Plan, accessed: 2024-08-24.

[10] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, "A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities," Sensors, vol. 22, no. 4, p. 1487, 2022.

[11] D. Drones, "FIX No Fly Zone, won't takeoff, DJI Drones," 2024, accessed: 2024-08-28. [Online]. Available: https://www.youtube.com/watch?v=nm5YdxXKV3E.

BRASÃO DE ARMAS DO REGIMENTO DE TRANSMISSÕES

Descrição Heráldica:

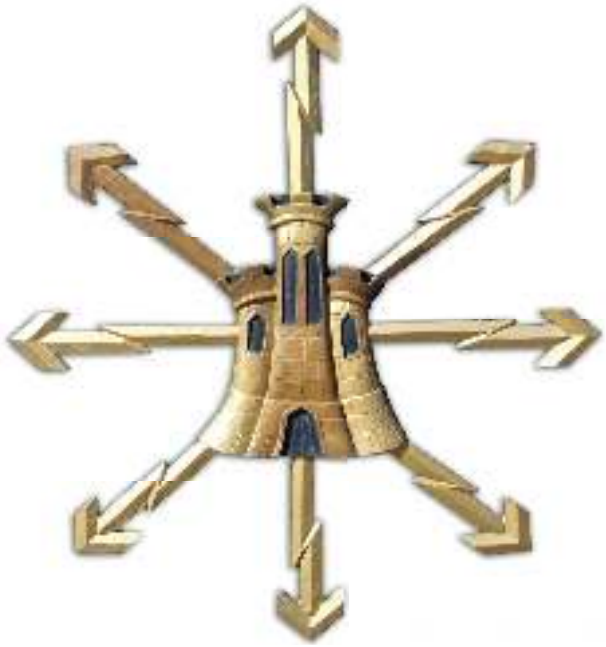
- Escudo de azul, numa almenara de ouro, iluminada e aberta de vermelho e acesa do mesmo perfilado de ouro;
- Elmo militar, de prata, forrado de vermelho, a três quartos para a dextra;
- Correia de vermelho, perfilada de ouro;
- Paquife e virol de azul e ouro;
- Timbre: uma garra de leão de vermelho empunhando seis raios elétricos de ouro;
- Divisa: num listel branco, ondulado, sotoposto ao escudo, em letras de negro, maiúsculas, estilo elzevir «SEMPRE MELHOR».

Simbologia e Alusões das Peças:

- A ALMENARA (torre de sinais) é símbolo heráldico das comunicações.

Representação e Significado dos Metais e Cobres:

- Ouro: sol, nobreza;
- Vermelho: fogo, energia criadora;
- Azul: ar, espaço, lealdade.



GRITO DAS TRANSMISSÕES

Na Vanguarda,

Avançamos

O Mundo,

Informamos

O Segredo,

Guardamos

As Transmissões,

Mantemos

Alfa, Bravo, Radiações
Bip, Bip, TRANSMISSÕES
Alfa, Bravo, Radiações
Bip, Bip, TRANSMISSÕES

REPÚBLICA PORTUGUESA

DEFESA NACIONAL

EXÉRCITO PORTUGAL