



mensagem



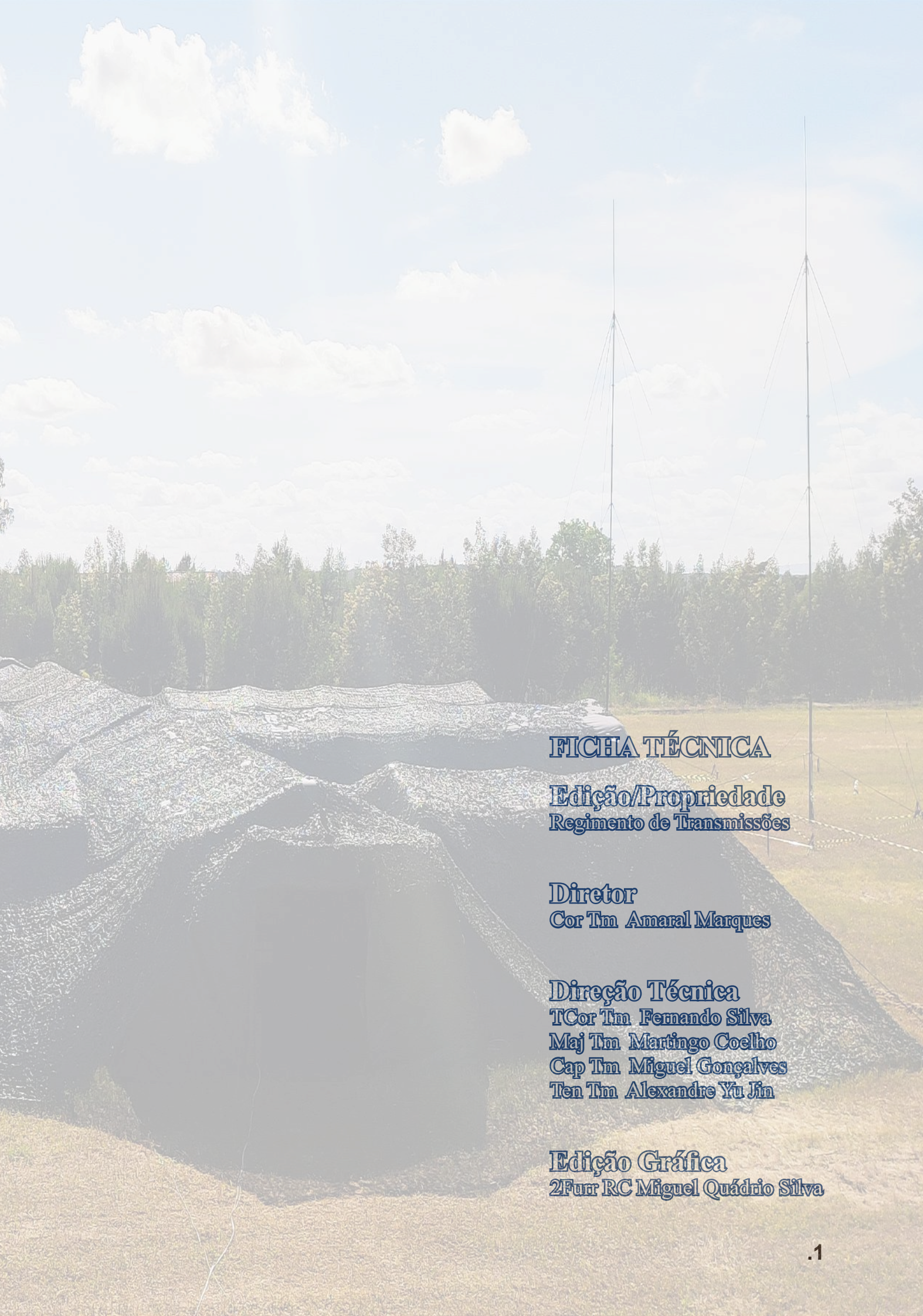

EXÉRCITO



Boletim Informativo
Regimento de Transmissões
Edição 2024

SUMÁRIO

• Editorial	2
• Mensagem do Diretor Honorário da Arma de Transmissões	4
• Entrevista ao Exmo. Major-General Viegas Pires	6
• Francisco António Ceira e o Corpo Telegráfico Português	12
• O Exército na edificação de uma capacidade nacional <i>Federated Mission Networking</i> (FMN)	20
• Exercício GOLFINHO 23	30
• A estruturação de um SOC – diferenças entre os SOC empresariais e o GOC do Exército	34
• Arquitetura Unificada de Comunicações para viaturas militares táticas	38
• Desenvolvimento Aplicacional: <i>On-premises vs Cloud</i>	40
• A Guerra de Informação porque é hoje mais importante que nunca?	42
• A relevância do CSO Alternativo na resiliência dos SIC do Exército e das Forças Armadas em geral	46
• Participação do Exército nas edições do SIRESP <i>Bootcamp</i>	52
• As comunicações no apoio de uma <i>Quick Reaction Force</i> no Teatro de Operações da República Centro Africana	54
• O Módulo CSI da 3ªFND CAatMec/ROU	56
• As Transmissões na Missão de Treino Portuguesa na República da Guiné-Bissau	58
• Principais atividades realizadas pelo RTm durante o ano de 2023	64
• Arma de Transmissões - Dados estatísticos relativos ao ano de 2023	68
• A Formação no Regimento de Transmissões	74
• 1.º Curso de Operações de Guerra Eletrónica	78
• Produção de Energia através de um Sensor de Movimentos acoplado a um Íman Permanente	82
• Extensão da rede RED a escalões táticos	88
• Técnicas de Calibração para um Novo Radar Espacial com Sistema de Direcionamento para Antena <i>Cassegrain</i>	96
• <i>Cluster</i> de características de eventos do <i>Windows</i> e <i>NetFlow</i> definidos dinamicamente para detecção de intrusões	104
• Distribuição Quântica de Chaves Portátil em Espaço Livre e Alta Velocidade	112



FICHA TÉCNICA

Edição/Propriedade
Regimento de Transmissões

Diretor
Cor Tm Amara! Marques

Direção Técnica
TCor Tm Fernando Silva
Maj Tm Martingo Coelho
Cap Tm Miguel Gonçalves
Ten Tm Alexandre Yu Jin

Edição Gráfica
2Furr RC Miguel Quádrio Silva



Editorial

É com grande satisfação que felicitamos por mais um aniversário todos os militares e civis que servem ou serviram na Arma de Transmissões e no seu Regimento. A Arma festeja 54 anos de existência e o Regimento 59 anos.

Como é tradição, coincide com mais um lançamento da revista “A Mensagem”, que pretende com a sua publicação preservar e partilhar informação, abordando conteúdo técnico, tático, experiências pessoais e reflexões. É nossa expectativa que os temas despertem curiosidade, discussão e promovam a aquisição de mais conhecimento aos nossos leitores.

Convido à leitura da nossa revista, que mantendo uma estrutura semelhante a anos anteriores, tem no seu início a mensagem do Exmo. Major-General Diretor Honorário da Arma de Transmissões, seguido de uma entrevista sua, aos Alferes-Alunos Tirocinantes. Depois é composta por um artigo que retrata um período histórico e as comunicações telegráficas, seguido de um conjunto de artigos, muito interessantes de ler, onde são descritas soluções tecnológicas para dar resposta a recentes capacidades do Exército.

Segue-se um conjunto de artigos que abordam a participação do Exército nas edições do “SIRESP Bootcamp” e as experiências vividas, na primeira pessoa, em Forças Nacionais Destacadas, em vários teatros de operações, como a República Centro-Africana e Roménia.

Após as experiências internacionais, regressamos ao RTm, onde se dá a conhecer um resumo das principais atividades do ano de 2023. No artigo seguinte são referidas as alterações da situação de pessoal relativas a todos os Oficiais e Sargentos do Quadro Permanente da Arma de Transmissões.

Quase a terminar, temos dois artigos, um sobre a formação ministrada no RIm e outro, especificamente, sobre o 1º Curso de Operações de Guerra Eletrónica.

Para terminar a nossa revista, temos um artigo sobre o trabalho desenvolvido no âmbito do concurso de energias renováveis relativo ao ano de 2023, realizado pelo EMGFA com o tema, “Energia para o Soldado” e os tradicionais artigos de investigação dos nossos Alferes-Alunos Tirocinantes que resultam das suas teses de Mestrado do Instituto Superior Técnico.

Mais um ano exigente decorreu, em que cumprimos a nossa missão com os encargos operacionais em exercícios e nos teatros de operações, ministramos e recebemos formação, realizamos atividades de divulgação do serviço militar, das Forças Armadas e do Exército e também ações de apoio ao desenvolvimento e bem-estar da população.

Estou confiante que, apesar dos desafios serem grandes, por um lado, a constante evolução tecnológica no Comando e Controlo e por outro, a falta de recursos nos quadros de pessoal da Arma, com a nossa elevada competência profissional e espírito de sacrifício, vamos continuar a cumprir com sucesso a nossa missão.

Agradeço a participação de todos os que contribuíram para a realização de mais uma edição da revista “A Mensagem” e saúdo todos os militares e civis da Arma de Transmissões, que contribuem ou contribuíram com “Engenho e Ciência”, num desígnio de Servir “Sempre Melhor”, o Exército e Portugal.

Bem hajam!

O Comandante do Regimento de Transmissões,

*António Luís de Paula Marques
(a. T. (a. T.))*



MENSAGEM DO DIRETOR HONORÁRIO DA ARMA DE TRANSMISSÕES

Major-General Viegas Pires

Mais uma vez, chegados a março, é no dia 24, dia do Arcanjo São Gabriel, padroeiro das Transmissões, que comemoramos o dia da nossa Arma. Este ano a Arma de Transmissões festeja o seu 54º aniversário.

Apesar da sua curta existência como Arma, no Exército, as Transmissões existem nas forças militares nacionais organizadas desde os primórdios da nacionalidade. Contudo, é durante as invasões francesas que as tropas de Transmissões surgem formalmente no Exército, com a criação do Corpo Telegráfico Militar, em 1810, anexo ao Real Corpo de Engenheiros. A nossa história tem assim raízes longínquas no tempo, ajudando-nos a entender o nosso passado, a viver o presente e a construir o nosso futuro.

Neste momento, quero aqui deixar uma palavra de apreço e reconhecimento a todos os que serviram nas Transmissões, que ajudaram a edificar a nossa história, e nos permitiram ser hoje quem somos, com uma identidade própria que nos caracteriza.

Uma saudação especial, igualmente, a todos os Quadros e Tropas de Transmissões (Tm) que servem e neste momento leem esta edição fora do Território Nacional (TN), com uma palavra de amizade e reconhecimento pela qualidade das funções que desempenham, extensível às respetivas famílias, incedíveis pilares de sustentação, para que todos possam diariamente dar o melhor de si, nas mais diversas missões e compromissos assumidos pelo Estado Português além-fronteiras.

Do mesmo modo, saúdo os militares de Tm e civis que servem em Território Nacional, nas diversas Unidades, Estabelecimentos e Órgãos do Exército, das Forças Armadas, da Guarda Nacional Republicana, em órgãos da administração direta e indireta do Estado, na Presidência da República e em Organizações Internacionais.

Neste ano que passou, a atividade das nossas unidades e órgãos foi particularmente preenchida.

Saliento que, desde 6 de junho de 2023, o Exército passou a contar com dois novos Órgãos de Base, da Arma, o Centro de Transmissões do Exército (CTE) e o Centro de Guerra da Informação e Ciberespaço (CGIC), ambos sediados em Lisboa, no quartel de Sapadores, sinal inequívoco da importância e confiança que o Comando do Exército deposita em todos quantos servem nas Transmissões.

O Batalhão de Transmissões (BTm) e as Companhias de Transmissões (CTm) da Brigada Mecanizada (BrigMec) e da Brigada de Reação Rápida (BrigRR), participaram nas Forças Nacionais Destacadas (FND), nos Teatros de Operações da República Centro Africana (RCA), contribuindo para o Comando e Controlo (C2) dessas forças com 14 militares em cada Teatro, desafio que esperamos poder vir a ser incrementado, participando igualmente neste esforço, ao nível das atividades ciber-eletromagnéticas, com militares da Companhia de Guerra Eletrónica (CompGE) e do Módulo Tático de Ciberdefesa do Exército.

No âmbito dos exercícios internacionais, salientam-se as seguintes participações: no *Coalition Warrior Interoperability Exercise 2023* (CWIX 23), com dez militares de Tm; no exercício internacional bilateral com Espanha, de interoperabilidade de comunicações e sistemas de informação, denominado de *Validación, Verificación y Confirmación Nacional de Federated Mission Networking* (V2CN – FMN), com a participação de cinco militares de Tm; no exercício internacional no âmbito do Projeto de Geminção entre a Brigada de Intervenção e a Brigada "Galicia" VII (BRILAT), no qual 8 militares do BTm participaram como observadores no exercício ÉGIDE 23; e no exercício internacional no âmbito do

Projeto de Geminação entre a BrigMec e a Brigada Mecanizada “Extremadura XI”, (BRIMZ XI), no qual 6 militares de Tm participaram, para testar a interoperabilidade entre rádios que equipam as Unidades de Escalão Batalhão e Companhia de ambos os países. Nos exercícios em território nacional, o Regimento de Transmissões, através do BTm, contribuiu para o aprontamento de forças para a RCA e para a Roménia, com cedência de material e afetação de pessoal, e participou ao longo do ano, através da CompGE, em sete exercícios, tendo a Direção de Comunicações e Informação (DCI) e o CGIC participado no planeamento e na execução da 13.^a edição do exercício do CIBER PERSEU, exercício de ciberdefesa do Exército, que reuniu mais de 50 organizações nacionais e participantes estrangeiros de 12 países, num total de participantes superior a 120 elementos, internos e externos às Forças Armadas.

Salienta-se ainda neste âmbito, a criação em março de 2024, de um novo exercício de comunicações do Exército (CISEX), tendo em vista treinar as componentes de Comunicações e de Sistemas de Informação dos diferentes Elementos da Componente Operacional do Sistema de Forças, constituindo-se as unidades e órgãos de Tm como facilitadores para a execução do mesmo.

Releva-se igualmente a presença da DCI em 2023 nas conclusões das jornadas da Chefia de *Sistemas de Información, Telecomunicaciones y Asistencia Técnica* do Exército de Espanha e no exercício VALIANT LYNX do NATO *Rapid Deployment Headquarters* (HQ NRDC-ESP).

O CTE apoiou a reestruturação da Rede de Dados do Exército, no Campo Super M’Poko na RCA, através da projeção de ferramentas, equipamento e cinco militares, e implementou, na sua capacidade operacional inicial, o Centro de Sistemas Operacional Alternativo, em Santa Margarida.

O Regimento de Transmissões, como Polo de Formação da Escola das Armas, assegurou durante o ano transato a realização de 32 cursos a 580 formandos, bem como a formação aos Cursos de Promoção a Cabo e de Praças, na Especialidade Comunicações.

Em termos de futuro próximo, face aos projetos de capacitação em curso, o Exército irá, durante 2024, incorporar um conjunto apreciável de material que permitirá um salto tecnológico notável nas respetivas áreas, com repercussões muito positivas ao nível do desempenho operacional das Transmissões e do Exército.

É assim, com orgulho, que o Diretor Honorário da Arma de Transmissões testemunha que a Arma, e todos quantos nela servem hoje, se constitui, cada vez mais, como um instrumento ímpar ao serviço do Comandante do Exército, para o eficaz acompanhamento, e respetiva eficiente incorporação nos assuntos militares, da acelerada evolução em curso ao nível de tecnologias emergentes, como a computação quântica e a biotecnologia aplicada à melhoria do desempenho do ser humano, e de tecnologias disruptivas, como a inteligência artificial, o big data, a hiper conectividade e os sistemas autónomos, de forma a assegurar ao Exército, e às Forças Armadas Portuguesas em geral, a indispensável preparação para permitir acompanhar o salto tecnológico para uma nova era, decorrente do previsível alcançar do período de convergência destas tecnologias, já em meados do segundo quartel deste Século XXI.

Apesar do elevado número de tarefas atribuídas ao Corpo Especial de Transmissões, e das implicações decorrentes da crescente exiguidade de recursos humanos que se tem vindo a verificar, fazendo jus à divisa da Arma – por Engenho e Ciência, temos demonstrado o nosso grande empenho individual e coletivo, elevada prontidão e competência, o que tem permitido atingir altos níveis de execução nas missões atribuídas, contribuindo decisivamente para um Exército cada vez mais credível, moderno e atrativo, estando por isso todos de parabéns.

Bem hajam!

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



Entrevista ao Exmo. Major-General Viegas Pires

Entrevista realizada pelos Oficiais Tirocinantes de Transmissões:

Alf Al Tm Daniel Almeida;

Alf Al Tm Ricardo Ferreira;

Alf Al Tm João Pinheiro;

Alf Al Tm Nilton Bárbara.

1. MEU GENERAL, QUE MOTIVOS O LEVARAM A ESCOLHER A CARREIRA MILITAR, MAIS CONCRETAMENTE A ARMA DE TRANSMISSÕES?

Sendo filho de militar e tendo nascido em Moçambique, durante uma comissão de serviço do meu pai, posso dizer que o contacto com o meio militar começou bastante cedo. Por este motivo, não é de estranhar que, quando acabei o liceu, tivesse decidido concorrer à Academia Militar.

Adicionalmente, as áreas de ciências, nomeadamente da eletrónica e da programação, foram sempre áreas que desde muito novo me despertaram interesse. Assim, a opção pelas Transmissões, uma das Armas mais tecnológicas do Exército, com uma grande base de engenharia eletrotécnica, quer nas vertentes comunicações e eletrónica, quer nas vertentes de sistemas de informação e computadores, foi sempre a minha primeira preferência.

2. DURANTE O SEU PERÍODO COMO COMANDANTE DO REGIMENTO DE TRANSMISSÕES, ENTRE 2008 E 2010, PODE PARTILHAR ALGUMAS ESTRATÉGIAS QUE IMPLEMENTOU PARA FORTALECER A EFICIÊNCIA E EFICÁCIA DA UNIDADE?

O Regimento de Transmissões (RTm), então sediado em Lisboa, no Quartel dos Quatro Caminhos, Sapadores, foi uma unidade onde passei grande parte da minha carreira militar. Primeiro como Capitão, tendo sido Comandante de Companhia (que chegou a ter mais de 300 efetivos, aquando da preparação da primeira força nacional destacada para Moçambique) e o último Chefe do Serviço Telegráfico Militar. Posteriormente, como Segundo Comandante, num período particularmente difícil em que o Exército deixou de ter Serviço Militar

Obrigatório, tendo o efetivo do Regimento passado a menos de metade do efetivo que tinha, com a saída das Praças que estavam nesse regime. Assim, quando fui escolhido para comandar o RTm, conhecia bem a unidade e assentei a minha ação de comando em três vetores que considerei essenciais: o vetor humano, com foco na liderança e na motivação do pessoal através da melhoria das infraestruturas, no incremento da formação e na constituição de equipas de trabalho mais dinâmicas e funcionais; o vetor logístico, com foco na gestão de cargas e no desenvolvimento de aplicações que permitiam controlar todos os equipamentos instalados nas redes do Sistema de Informação e Comunicações Operacional do Exército (SIC-OP) e apoiar na respetiva operação e manutenção; o vetor financeiro, com foco na capacitação dos respetivos intervenientes e na implementação prática dos novos procedimentos da contratação pública, tendo em vista a eficiência, eficácia e transparência de todos os processos administrativos e financeiros, ao nível regimental.

Considerando que um dos aspetos importantes também é dar a conhecer o que fazemos e partilhar conhecimento, dei orientações para ser criada a revista regimental, a Almenara, cujas edições anuais foram muito apreciadas e uma excelente forma de partilhar conhecimento, experiências e divulgar as diferentes atividades do RTm, em prol das Transmissões e do Exército.

3. COMO DIRETOR TÉCNICO DO PROJETO DE DESENVOLVIMENTO DO NOVO RÁDIO NACIONAL (P/GRC 525), QUAIS FORAM OS DESAFIOS TÉCNICOS E ESTRATÉGICOS ENFRENTADOS?

Na altura em que fui Diretor Técnico do projeto o cargo estava atribuído ao Chefe da Secção Logística da então Direção dos Serviços de Transmissões, localizada no Comando da Logística.



Foi um período bastante desafiante, na medida em que o projeto já durava há alguns anos, durante esse período tinham ocorrido algumas evoluções tecnológicas que necessitavam de ser integradas no equipamento, o rádio já se encontrava na fase final do seu desenvolvimento e procediam-se aos testes de aceitação para futura receção e entrada em funcionamento no Exército. Na altura, contávamos com uma equipa específica, do Exército, criada para realizar essa função e que reportava para o Diretor do Projeto. Em complemento foram enviados equipamentos para as unidades operacionais das Brigadas, a fim de serem testados. A conjugação das diferentes atividades permitiu melhorar o produto final, em muitos aspetos, como nos alcances, transmissão de dados, estanquicidade do equipamento e informação disponível no painel de comando do equipamento. Relativamente a este último ponto, lembro-me que o rádio não dispunha de indicador de carga da bateria que posteriormente foi incorporado no painel de comando e que era uma questão básica que não tinha sido considerada no projeto inicial. No âmbito destas atividades, foi ainda criada uma comissão de acompanhamento, que contava com elementos técnicos e de direção, quer da parte do exército, quer da parte da empresa responsável pelo desenvolvimento do rádio e que foi fundamental para a resolução dos vários problemas encontrados.

4. DURANTE A SUA LONGA CARREIRA DE 44 ANOS DE SERVIÇO, COMO CARACTERIZA A EVOLUÇÃO DAS TRANSMISSÕES NO NOSSO EXÉRCITO, EXISTEM PONTOS MARCANTES NESTA EVOLUÇÃO? SE SIM, QUAIS?

A Arma de Transmissões, com pouco mais de meio século de existência formal no Exército, tem tido momentos altos e baixos ao longo das diferentes épocas. Como aspetos menos bons, destaco a falta de investimento, nalguns períodos, que levaram a alguma estagnação na capacidade de apoio, quer no âmbito das comunicações, quer no âmbito

da guerra eletrónica.

Igualmente, o fim da capacidade informática que detínhamos, no Centro de Informática do Exército, e que, ao contrário dos outros Ramos, extinguimos com transferência de todo o “*Know how*” para o Ministério da Defesa, deixou uma lacuna importante ao nível dos desenvolvimentos específicos do Exército.

Não obstante, o aspeto mais negativo relaciona-se com a falta crescente de efetivos, que não é específico das Transmissões, pois afeta todo o Exército em geral, que é fundamental reverter, estando em curso um conjunto de medidas que se espera venham a mitigar esta situação.

Apesar da falta de investimento referida, a arma assistiu, ao longo deste últimos 40 anos, a momentos altos e marcantes da evolução das Tm no Exército, como a introdução das famílias de rádios 425 e posteriormente 525, das cabines de transmissões nos anos 80, dos equipamento de feixes hertzianos FM 200 e da remodelação do sistema telegráfico e posterior implementação da rede de dados do Exército. Seguindo este caminho de modernização e atualização, concretizámos a implementação do Sistema de Informações e Comunicações Tático (SIC-T), do Sistema de Informação Comando e Controlo do Exército (SICCE), a modernização do Sistema de Informação e Comunicações Operacional (SIC-OP), a implementação do Sistema Integrado de Controlo de Acessos e Videovigilância do Exército (SICAVE), o desenvolvimento do primeiro módulo tático de *Computer Incident Response Capability* (CIRC), que contribuiu para que o Exército fosse o primeiro Ramo a ter uma capacidade tática, no âmbito da ciberdefesa. Igualmente, voltámos a criar uma área, no âmbito da Informática, para apoio aplicacional ao Exército.

Recentemente, implementámos o *Battlefield Management System* (BMS), e estamos a incrementar as “Combat Net Radio” (CNR).



Atualmente, encontramos-nos, mais uma vez, num momento de transformação e atualização, como o desenvolvimento do projeto do soldado digital e esperando-se, a breve trecho, a introdução, no Ramo, de novos módulos do SIC-T e novos meios de Guerra eletrónica.

5. TENDO EM CONTA O ATUAL PAPEL DA NOSSA ARMA NAS OPERAÇÕES MILITARES, CONSIDERA QUE O INVESTIMENTO DO EXÉRCITO NAS TRANSMISSÕES É O SUFICIENTE? DE QUE FORMA ALOCARIA RECURSOS PARA O MELHOR APROVEITAMENTO DAS TRANSMISSÕES?

A Arma de Transmissões é uma Arma de apoio ao Comando e Controlo. Assim, destacam-se o apoio de comunicações, o apoio de guerra eletrónica e recentemente os apoios nas áreas da cibersegurança e ciberdefesa. De um modo geral, apesar de alguns constrangimentos experienciados, a Arma sempre tem sido capaz de levar a carta a Garcia, apoiando as unidades e o Exército, nas suas diferentes missões.

A integração de novos equipamentos e sistemas, como os referidos no ponto quatro anterior, permitirá manter os apoios pelos quais somos responsáveis. Contudo, é importante referir que muitos dos constrangimentos referidos anteriormente não têm origem internamente mas dependem de orientações externas.

Um dos recursos com que mais teremos de nos preocupar são os recursos humanos. Hoje assistimos a uma redução drástica de praças, sargentos e oficiais. Vários fatores são importantes para contrariar essa situação, encontrando estratégias ao nível da admissão, motivação e retenção de quadros. Estas estratégias terão de passar pela criação de melhores condições estatutárias e financeiras.

É também importante que os militares de Transmissões tenham um percurso variado, por vezes nas áreas mais técnicas e outras vezes em áreas operacionais. É evidente que tal depende do

respetivo quadro em que se encontram. Por exemplo, os oficiais da Academia Militar devem passar por atividades técnicas mas também operacionais, sendo as funções de comando fundamentais para a progressão desses militares.

Outras estratégias poderão passar por contratar pessoal técnico específico, para determinadas funções, libertando os quadros de transmissões para a sua atividade principal, no âmbito do apoio ao comando e controlo.

6. OLHANDO PARA O FUTURO DA ARMA DE TRANSMISSÕES, QUE MEDIDAS SUGERE PARA MANTER A ARMA ATUALIZADA FACE AOS AVANÇOS TECNOLÓGICOS EMERGENTES E ÀS EXIGÊNCIAS OPERACIONAIS EM EVOLUÇÃO?

A inovação e modernização tecnológica sempre influenciaram e irão continuar a influenciar a atuação dos exércitos. Equipamentos, organização, emprego de forças e doutrinas evoluem sob essa influência. As Transmissões, com um cariz fortemente tecnológico, são facilmente afetadas pelos desenvolvimentos nestas áreas.

Quer as comunicações, quer a guerra eletrónica continuarão a evoluir e a necessitar de acompanhamento e modernização. Contudo as áreas da cibersegurança e da ciberdefesa serão aquelas que, ao nível das Tm, mais atenção irão necessitar, por serem domínios novos em franco desenvolvimento.

Também ao nível das tecnologias, destaca-se a Inteligência artificial, que constituirá um desafio importante, na medida em que irá integrar a maioria dos sistemas futuros apressando a obsolescência tecnológica dos sistemas atuais.

Deste modo, como sempre, é fundamental acompanhar estas evoluções tecnológicas, desenvolver doutrinas em concordância com essas evoluções e integrar os novos equipamentos e sistemas, nos vários domínios da nossa atividade, para garantir a eficiência e eficácia dos apoios de Tm às atividades operacionais e ao Exército em geral.



7. DADA A SUA EXPERIÊNCIA INTERNACIONAL, ESPECIALMENTE EM ANGOLA E ESPANHA, PODERIA PARTILHAR ALGUMAS LIÇÕES APRENDIDAS E CONTRIBUIÇÕES PARA A COOPERAÇÃO E DESENVOLVIMENTO NAS RELAÇÕES BILATERAIS E INTERNACIONAIS?

Ao longo da minha carreira tive o privilégio de ser nomeado para cargos e funções fora do país.

O primeiro cargo que desempenhei, no exterior, foi como conselheiro na DELNATO, em Bruxelas. Foi um período bastante interessante, na medida em que me permitiu não só ter uma imagem da vertente militar da OTAN, bastante completa, mas também da vertente civil.

Como conselheiro militar do Exército tinha a cargo vários pelouros com destaque para o cargo de NADREP, sendo o representante do Diretor Nacional de Armamento (DNA) na Aliança. Além dessa função, tinha representação no Executive Working Group (para a área dos mísseis), no NATO-Russia Council Theater Missile Defense, no Civil Budget Committee, no Advisory Group of Financial Counselors e no Small Arms and Light Weapons. Adicionalmente, fui nomeado representante do DNA na European Defence Agency (EDA), no âmbito da União Europeia (UE). O desempenho destas atividades permitiu ter uma visão alargada das áreas do armamento e equipamentos de defesa da OTAN e da UE. Um dos aspetos menos positivo, que referenciei, foi o da pouca participação das indústrias de defesa nacionais nos projetos da Aliança, que contrastava com a forte representatividade das indústrias das restantes nações.

Em Angola fui o Diretor Técnico do Projeto de Cooperação para a Instalação e Funcionamento do Instituto Superior Ensino Militar (ISEM).

O ISEM ministrava cursos aos militares dos três Ramos das forças armadas angolanas como os cursos de promoção a oficial superior, de estado-maior e de promoção a oficial general.

O projeto contava com uma equipa docente residente em Luanda, responsável pelo apoio à dire-

ção de ensino e à ministração dos cursos, desde o planeamento à execução. Este núcleo permanente era reforçado, com docentes militares, dos três Ramos das forças armadas portuguesas, que se deslocavam a Angola para ministrar módulos específicos e, adicionalmente, participavam palestrantes civis, de universidades e instituições portuguesas.

Foi o contacto com uma realidade diferente mas que permitiu compreender a grande importância das forças armadas portuguesas para o desenvolvimento de relações de cooperação, em especial com os Países Africanos de Língua Oficial Portuguesa.

Por último, fui escolhido para o cargo de segundo comandante do Quartel-general do NATO Rapid Deployable Corps (NRDC HQ), em Valência, Espanha.

A OTAN conta com uma estrutura de comando *common funding* e uma estrutura de forças cujo financiamento é maioritariamente suportado pelas nações participantes. O NRDC HQ insere-se nesta última estrutura e tem a Espanha como *Framework Nation*, à qual se juntaram mais 11 nações (Alemanha, Estados Unidos da América, França, Grécia, Itália, Polónia, Portugal, Reino Unido, República Checa, Roménia e Turquia). De acordo com as diretivas OTAN participa num conjunto diversificados de exercícios e operações.

A participação em estruturas deste tipo confere aos militares a oportunidade de exercer funções operacionais, em ambiente diversificado, multifuncional, multicultural e multinacional, sendo uma mais-valia para a sua evolução técnico profissional. Foi, do ponto de vista pessoal e profissional, um dos momentos mais interessantes da minha carreira militar.

A participação de Portugal no HQ NRDC é importante não só pela contribuição que temos de dar para a Aliança como para o fortalecimento das relações bilaterais com Espanha. Sou da opinião que, tendo Portugal o lugar de *Deputy Commander*, deveríamos incrementar a nossa representação neste quartel-general.



É importante não esquecer que um militar é um representante do seu país. Quando no estrangeiro essa representação é mais evidente. A competência profissional demonstrada e o saber fazer e estar são os nossos melhores trunfos. Em geral, os militares portugueses são excelentes profissionais e são muito bem vistos quando desempenham missões no exterior o que traduz a excelente qualidade dos nossos quadros.

8. COMO DIRETOR HONORÁRIO DA ARMA DE TRANSMISSÕES, PODERIA DESTACAR ALGUMAS INICIATIVAS OU PROJETOS QUE TENHA PROMOVIDO PARA PRESERVAR A TRADIÇÃO E IMPULSIONAR O DESENVOLVIMENTO CONTÍNUO DA ARMA?

Com a extinção das Direções das Armas e Serviços, desapareceu a figura do respetivo diretor. Em consequência foi criada a figura dos diretores honorários. O Diretor Honorário da Arma de Transmissões (DHAT) é o responsável por continuar a preservação das especificidades, tradições e história das Transmissões. Desta forma o DHAT passou a ser o fiel depositário da história e cultura da Arma, dinamizador do respetivo espírito de corpo e representante protocolar da Arma e do respetivo quadro especial.

Sendo o responsável por assessorar o comando do Exército no âmbito das atividades referidas e pela apresentação do plano anual das atividades da Arma ao Exmo. General CEME, para aprovação, e a fim de contribuir para o desenvolvimento da coesão e do espírito de corpo dentro da Arma, integrei todas as atividades festivas das unidades das Transmissões no respetivo planeamento e inclui dois eventos semestrais, com vista à partilha de conhecimentos e experiências, entre elementos com responsabilidades no âmbito das atividades de transmissões, em contextos internos e externos ao Exército. Igualmente, incentivei e apoiei a elaboração de publicações, com vista à preservação da memória das Tm, como a obra referente aos cinquenta

anos das transmissões, em dois volumes, publicada durante as festividades do cinquentenário das Transmissões, em 2023, e a elaboração da obra “As Transmissões Na Grande Guerra”, da autoria do Coronel Aniceto Afonso que será lançada este ano.

9. COMO ACESSOR DO CHEFE DO ESTADO-MAIOR DO EXÉRCITO PARA A MODERNIZAÇÃO E INOVAÇÃO, PODE PARTILHAR ALGUMAS DAS SUAS CONTRIBUIÇÕES PARA PROMOVER A MODERNIZAÇÃO NAS FORÇAS ARMADAS?

Quando fui convidado para Assessor do CEME para a Modernização e Inovação do Exército tive como missão desenvolver um conjunto de atividades com vista à implementação de uma unidade que desenvolvesse a sua atividade nas áreas da inovação, modernização e experimentação operacional do Exército.

Foi uma missão muito gratificante que permitiu levantar, em conjunto o Estado-maior do Exército, Órgãos Centrais de Administração e Direção, Comando das Forças terrestres, Academia Militar e Direção de Finanças, um inventário alargado do conjunto de competências existentes no Ramo e desenvolver as bases para a criação do Centro de Experimentação e Modernização Tecnológica do Exército (CEMTEEx), em termos de efetivos, *job description* para cada cargo, estrutura da unidade, necessidades de interação com entidades externas (como universidades, centros de investigação e indústrias de Defesa), localização, infraestruturas e missão da unidade.

Deste modo, é com muito agrado e sentimento de missão cumprida que hoje vejo o CEMTEEx, localizado em Paço de Arcos, e inaugurado em 20 de outubro de 2022.



10. DE TODOS OS CURSOS QUE TIROU EM TERRITÓRIO NACIONAL E ESTRANGEIRO, QUAIS FORAM OS MAIS IMPORTANTES PARA A SUA CARREIRA E EM QUE MEDIDA?

Ao longo da minha carreira, frequentei e conclui uma grande variedade de cursos, realidade que é comum aos militares das forças armadas que, dentro do Estado, são dos que mais tempo passam em atividades de formação. Efetivamente, muitos de nós frequentamos, ao longo das nossas carreiras, além dos cursos de formação e promoção obrigatórios, outros cursos e estágios de capacitação ou qualificação quer militares, quer civis, nacionais e/ou internacionais.

Se tivesse que priorizar os cursos que fiz, destacava quatro deles, pese embora, o facto de todos eles terem a sua importância e o seu momento e terem contribuído para o profissional que sou hoje.

Em primeiro lugar, destaco o curso da Academia Militar, Curso de Ciências Militares das Armas, na especialidade de Transmissões, que me permitiu ser oficial de Transmissões do Exército.

Em segundo lugar, o curso de Engenharia Eletrotécnica e de Computadores, pré Bolonha, do Instituto Superior Técnico, que me permitiu ter as bases de engenharia que considero fundamentais para a atividade técnica de todos os oficiais da Arma e que completei com o mestrado Integrado, pós Bolonha, em Engenharia Eletrotécnica Militar, na especialidade de Transmissões. Atualmente o curso de Tm da AM confere o grau de mestre em engenharia eletrotécnica militar. Esta situação, que não é comum nos Exércitos ocidentais da OTAN, permite conferir, aos oficiais da Arma de Transmissões do Exército português, uma variedade de competências, que os habilitam a desempenhar um conjunto alargado de missões, constituindo uma mais-valia para o Ramo.

Em terceiro lugar, destaco o curso de Estado-maior, tirado no antigo Instituto de Altos Estudos Militares, que considero fundamental para qualquer militar e que foi muito útil, ao logo da minha carreira,

quer nas funções que desempenhei em território nacional quer nas que desempenhei no exterior.

Por fim, destaco o *Collège Interarmées de Défense*, em França. Um curso que integra alunos dos três Ramos das forças armadas, *gendarmérie* e civis da área da defesa onde, além de outras matérias, me foi permitido conhecer de perto as forças armadas francesas, respetivas doutrinas, organização e equipamento, abrindo horizontes e incrementando competências no âmbito técnico profissional que muito contribuíram para o desempenho de funções internacionais.

11. MEU GENERAL, QUE RECOMENDAÇÕES/SUGESTÕES DARIA AOS NOVOS OFICIAIS DA ARMA DE TRANSMISSÕES?

Acima de tudo é importante estarmos motivados e gostarmos do que estamos a fazer.

É importante conhecer bem a instituição em que estamos inseridos.

Ao longo da nossa carreira militar, devemos compreender o ambiente envolvente e saber o que se espera que façamos, em cada momento das nossas vidas. Tal implica uma necessidade de mantermos um esforço na nossa formação e respetiva atualização e procurarmos fazer sempre o melhor possível, em função dos objetivos traçados e das missões que em cada momento nos forem atribuídas, imbuídos dos princípios, qualidades e virtudes que caracterizam os militares.

As Transmissões são uma família coesa. Estamos unidos pelo espírito de corpo cimentado pela transversalidade de gerações que serviram e servem na Arma.

Todos nós somos elementos importantes e fundamentais para que a Arma se afirme no Exército.

Assim, felicito os novos oficiais da Arma, pela escolha que fizeram, ao entrar no quadro especial de Transmissões.

As Transmissões, o Exército e o País contam convosco.



Francisco António Ciera e o Corpo Telegráfico Português

Do Início da Telegrafia Óptica ao Fim das Guerras Peninsulares (1803-1814)

Sargento-Chefe Tm Paulo Costa

Sargento de Materiais na Repartição de Museus

Introdução

Historicamente, as primeiras comunicações à distância, consistiam apenas na transmissão e receção de sinais simples de modo a que o inimigo não pudesse identificar a mensagem a transmitir. Fernão Lopes [1] nas suas crónicas, menciona a utilização de almenaras, pequenas torres situadas em locais elevados e com visibilidade entre elas, permitindo durante o dia com fumo e à noite com fogo, emitir sinais através de meios visuais. Assim, até ao início do Séc. XIX, uma grande parte da informação ainda era difundida por mensageiros, após esta data surge pouco a pouco um novo meio de comunicação em Portugal, a telegrafia visual.

1. Francisco António Ciera (1763-1814)

Francisco António Ciera [2] nasceu em Lisboa em 1763, filho do matemático italiano Miguel António Ciera e de Antónia Margarida Violante de Lima, portuguesa. Em 1790 iniciou trabalhos de geodesia em Portugal, liderando a “Comissão Geodésica” a fim de obter a triangulação geral do país com o objetivo da construção da Carta do Reino. Em 02 dezembro de 1803 foi nomeado Diretor da Rede da Barra [3] e em 12 de junho de 1803 foi encarregue de dirigir as comunicações telegráficas visuais [4].



Fig. 1 - Francisco António Ciera

Francisco Ciera veio a construir o telégrafo óptico de ponteiro português em 1808, sendo muito mais simples e económico do que qualquer outro existente à época [5]. O seu conhecimento em cartografia, levou a que o Príncipe Regente o nomeasse com o objetivo de introduzir mudanças na Rede da Barra.

Em 1813 Ciera adoece, e em 1814 veio a faleceu em Lisboa. A sua longa experiência cartográfica permitiu-lhe visitar inúmeros locais no país e utilizar diversos tipos de equipamentos topográficos, que lhe foram mais tarde úteis para a criação dos novos equipamentos telegráficos.

Saliente-se ainda o facto de que Francisco António Ciera não era militar.

[1] - Escrivão e cronista oficial do Reino (Lisboa 1385- Lisboa 1460).

[2] - LIMA, MGen António Luís Pedroso de; AFONSO, Cor. Aniceto; ALVES, MGen Carlos; DIAS, Cor. Jorge Costa; Bicentenário do Corpo Telegráfico 1810-2010; Edição da Comissão Portuguesa de História Militar; Comissão da História das Transmissões; Grafismo: Blueprint, Lda; Impressão: Palmigráfica; ISBN nº 978-989-95946-3-0; Lisboa 2010; Pág. 25.

[3] - Rede de comunicação telegráfica visual existente, entre o Cabo da Roca e o Castelo de S. Jorge.

[4] - AHM/DIV 1/16/048/37 m 0042.

[5] - Ciera apresenta a comparação do seu telégrafo com os telégrafos que existiam à época, o francês de Chappe, o sueco de Edelcrantz e o inglês de Murray. Carta de Ciera de 25out1808. AHM DIV 1-14-170-07.



1.1 Sistema óptico

Nos finais do Sec. XVIII, foram feitos progressos significativos no desenvolvimento de novos meios de comunicação à distância, desta feita, surge então o telégrafo óptico Francês pela mão dos irmãos Chappe. Este foi utilizado pela primeira vez em 1792 entre Paris e Lille, cobrindo uma distância de cerca de 230 km.

Este tipo de equipamento foi implementado mais tarde em Portugal para as comunicações a longas distâncias, utilizando um conjunto de estações situadas em locais elevados e com visibilidade entre elas com distâncias não superiores a 12 km em média. Cada estação dispunha de um dispositivo de transmissão de sinais, que obedecia a códigos pré-estabelecidos. O operador da estação emissora enviava os sinais através da telegrafia visual, o operador da estação receptora, através do uso de um óculo, recebia a mensagem enviada e reenviava-a novamente para a estação seguinte e assim sucessivamente até à estação final. Os operadores intermédios, não teriam a necessidade de conhecer o conteúdo da mensagem, que era destinada exclusivamente aos destinatários finais. Este sistema era muito eficaz, no entanto apresentava dificuldades de transmissão, sobretudo com falta de visibilidade ou à noite [6].

1.2 Telégrafo de Ponteiro

O telégrafo de ponteiro era prático e simples de operar, ideal para as operações de campanha. O operador acionava uma manivela, permitindo o movimento a um ponteiro colocado uns metros acima do operador [7]. O ponteiro dispunha de oito posições, que correspondiam a 0=1,2,3,4,5,6, estas associadas com as “táboas telegráficas” poderiam reproduzir milhares de combinações possíveis, correspondendo cada uma delas a uma letra, palavra ou frase.

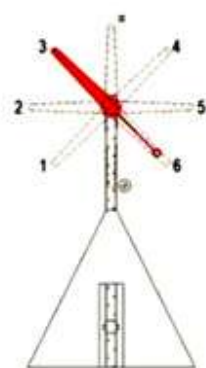


Fig. 2 - Telégrafo de Ponteiro

[6] - VEGAR, José; Vencer a distância - Percurso das Comunicações em Portugal; Museu das Comunicações; Fundação Portuguesa das Comunicações; Design: Arne Kaiser; Impressão Loures Gráfica. SA.

[7] - "...tinha uma só manivela com a qual se dá ao seu único ponteiro as inclinações de 45° em 45° em relação ao mastro principal; de sorte que um só homem observa, faz os sinais e escreve tudo a um tempo pois tem a vista aplicada a uma luneta fixa no mastro, move a mão esquerda ficando com a direita livre para escrever numa pedra convenientemente aplicada ao mastro para esse fim". AHM DIV 1-14-170-07.



1.3 Telégrafo de persianas

O Telégrafo de Palhetas era constituído por um conjunto de três persianas retangulares de madeira, que podiam ser colocadas na posição vertical ou horizontal, permitindo assim também oito posições de trabalho e as respectivas combinações[8]. Este tipo de telégrafo seria utilizado inicialmente para curtas distâncias, talvez inferiores a 12 Km, mas a sua eficácia manteve-o ao serviço durante mais de 40 anos.



Fig. 3 - Telégrafo de persiana

SÍMBOLO	ESQUEMA	Observações	
○		Persianas todas abertas	
■		Persianas todas fechadas	
1		Uma persiana aberta	
2			
4			
3		1 2	Duas persianas fechadas
5		1 4	
6		2 4	

Fig. 4 - Código do Telégrafo de persiana

1.4 As Instruções para o serviço, códigos e “Táboas telegráficas”

Na telegrafia visual, o texto de uma mensagem era convertido em código de acordo com as “taboas telegráficas” que o telegrafista emissor transmitia à estação seguinte até ao final. Após a recepção final, o destinatário teria que decifrar novamente o texto enviado e de acordo com os códigos estabelecidos. Os operadores intermédios não teriam a necessidade de decifrar o texto, sendo também uma forma de manter segura a informação.



Fig. 5 – Pagina 4 e 5 das “Taboas telegráficas”

[8] - As palhetas correspondiam aos números 1, 2 e 4. Quando as palhetas se apresentavam na vertical somavam-se os números respetivos. Podiam-se representar os números de 1 a 7 e o zero (0) que dava 8 posições. Como o 0 e o 7 eram reservados para serviço ficavam 6 para transmissão de mensagens.



O sistema criado por Ciera era baseado nos códigos das “táboas telegráficas” [9]. Estas continham 90 páginas com cerca de 10. 000 [10] entradas com números, letras ou palavras. Se alguma palavra não constasse da lista inicial, poderia ser enviada letra a letra. A primeira página do documento continha letras do alfabeto e na página seguinte a numeração. As páginas quatro e cinco apresentavam artigos, pronomes e palavras correntes, e da página seis em diante, apresentava conjuntos de palavras, apresentadas por ordem alfabética sendo as páginas finais destinadas às localidades. O sistema de transmissão permitia simplicidade e rapidez, evitando percas de tempo assim como os erros de transmissão.

1.5 Rede da Barra

A Rede da Barra não teve alterações significativas até 1803, ano em que é estabelecida a primeira rede de telegrafia visual propriamente dita. Esta estendia-se desde o Farol do Cabo da Roca ao Castelo de S. Jorge, destinando-se essencialmente ao controlo marítimo e aduaneiro [11] das embarcações que entravam ou saíam no Tejo. As distâncias entre estações não ultrapassavam em média os 3 Km. Ciera estipulou que apenas a Torre de Belém comunicava com as embarcações, e que os sinais utilizados se faziam com emprego de um mastro onde se içariam bandeiras ou balões em sobreposição à utilização do telégrafo de bandeiras [12].

Com a melhoria da rede de comunicações, fez-se aumentar as distâncias entre estações possibilitando assim reduzir o seu número.

1.6 A Telegrafia Visual da Casa Real

A telegrafia óptica atraiu um enorme interesse por parte do Príncipe Regente, chegando a solicitar a instalação de um equipamento no Palácio de Mafra, e de modo a que o pudesse ver e manipular [13].

Em 1807, antes da saída da família real para o Brasil devido á invasão de Junot, Ciera manteve em funcionamento um telégrafo exclusivamente para o Príncipe Regente. Este telégrafo, estava associado a uma rede que ligava Lisboa a Mafra, Queluz, Torre de Belém e S. Julião da Barra, mantendo-se em funcionamento mesmo depois da saída da família real para o Brasil. Esta rede permitiu também que a corte se mantivesse informada acerca do que ia acontecendo no resto do país.

1.7 Rede e Estações telegráficas

Terminada a primeira invasão, e após a saída das tropas francesas do nosso território em 1808, surgiu a oportunidade de alargar a rede telegráfica, tendo como objetivo a segurança e defesa do país.

Em dezembro de 1808, Ciera apresentou uma proposta de orçamento para o alargamento da rede telegráfica, planeando que estivesse concluída após seis meses depois do início dos trabalhos. A execução da obra estaria a cargo do TGen Pedro Folque [14], tendo-se iniciado os trabalhos em princípios de 1809.

[9] - Nas “táboas” eram utilizadas todas as combinações dos algarismos 1 a 6, sendo o número mais elevado 66 666.

[10] - Tinha 9 720 entradas com 108 letras, palavras ou frases.

[11] - FONSECA, Moura da; *As comunicações Navais e a TSF na Armada*; 1988, pág. 30.

[12] - Quando Ciera introduziu o telégrafo português na Rede de Barra, apenas a estação da Torre de Belém comunicava com os navios no rio Tejo.

[13] - Carta datada de 1807 existente no AHM, Cota DIV-1-14-170-07.

[14] - TGen (Stays – Catalunha, 30abr1744 – Lisboa, 06abr1848). Colaborou com Francisco Ciera na elaboração da carta topográfica de Portugal. Pertenceu ao Real Corpo de Engenheiros. Autor do Dicionário Militar (1827) com o registo dos sinais telegráficos da época.



A Rede de Abrantes estaria em funcionamento em novembro desse mesmo ano de 1809, e a Rede de Elvas entrou em funcionamento em fevereiro do ano seguinte [15]. Em 1810/11, além da rede costeira entre Lisboa e o Cabo da Roca, existiam mais três redes em funcionamento permanente ou temporariamente.

A Rede Lisboa-Almeida era estratégica, ramificava em Santarém para Elvas e na Atalaia para Abrantes, pontos-Chave para a defesa do território. A extensão total seria da ordem dos 500 Km, e era constituída por 25 estações, sendo guarnecida por 82 homens [16]. A distância média entre estações seria da ordem dos 18 km, no entanto esta distância podia chegar aos 40 Km (Almeirim a Montargil). Para comunicar a estas distâncias seriam necessários enormes telégrafos de persianas, assim como a utilização de sofisticados meios de observação, com a capacidade de ampliação na ordem das 30 a 40 vezes.



Fig. 6 - Diagrama da Rede Telegráfica

2. O Corpo Telegráfico

Da criação ao Final da Guerra Peninsular (1810-1814) [17]

2.1 Corpo telegráfico

O Corpo Telegráfico foi criado em 05 de março de 1810 [18]. Este Corpo tornou-se responsável pela rede telegráfica existente, dependia do Ministério da Guerra e tinha um efetivo de cerca de 100 militares, sendo o seu primeiro Diretor Francisco António Ciera.

Também em 1810, foi impresso em Lisboa a “Organização, e Regulamento de Disciplina do Corpo Destinado ao Serviço dos Telégrafos” definindo as normas de funcionamento do Corpo Telegráfico.

O efetivo do Corpo Telegráfico seria da ordem dos 120 homens, no entanto o seu número foi oscilando, aumentando durante a ocupação francesa e descendo depois dela. Compreendia o seu Diretor-Geral, 6 Oficiais Primeiros-Ajudantes, 3 Segundos-Ajudantes, 17 Primeiros-Cabos, 28 Segundos-Cabos e 54 Soldados. A seleção destes militares era efetuada entre os oficiais inferiores e soldados de linha, reformados, hábeis para o serviço e conduta regular [19].

As punições, quando aplicadas a estes militares, eram pecuniárias com a perda do seu vencimento. Este sistema implicava que os operadores tivessem que aplicar todo o seu zelo e aptidão ao desempenho do seu serviço, evitando falhas. Em último caso, os militares não cumpridores poderiam ser expulsos.

[15] - AHM/div/3/32/1/64, relação de 12abr1810 e AHM/FG5/8/294/livro 1718/aviso nº 294 de 15mai1810.

[16] - AHM 3º div, 32ª secção, caixa 1 nº 64.

[17] - SANTOS, General Garcia dos; PINTO, TGen Pereira; LIMA, MGen Pedroso de; GOLIAS, TCor Jorge; Comissão da História das Transmissões; As Transmissões Militares da Guerra Peninsular ao 25 de Abril; Coordenação: AFONSO, TCor Aniceto; Colaboração: FALCÃO, Cor. Carlos; DIAS, Cor. Costa; CANAVILHAS, Cor. Lopes; Gráfica Blueprint, Lda; Impressão Gráfica: Europam, Lda.; Lisboa 2008.

[18] - MACEDO, Coronel Tm (Engº) Henrique José da Silva Castanheira; Regimento de Transmissões: 30 Anos de Serviços Distintos 1977-2007; Coordenação: RIBEIRO, Tenente-Coronel Tm (Engº) Carlos Jorge de Oliveira; Redação e Edição Estado-Maior do RTm; Batalhão de Comunicações e Sistemas de Informação, Centro de Segurança da Informação; Propriedade Regimento Transmissões; Impressão: M2; 14 setembro 2007..

[19] - LIMA, MGen António Luís Pedroso de; AFONSO, Cor. Aniceto; ALVES, MGen Carlos; DIAS, Cor. Jorge Costa; Bicentenário do Corpo Telegráfico 1810-2010; Edição da Comissão Portuguesa de História Militar; Comissão da História das Transmissões; Grafismo: Blueprint, Lda.; Impressão: Palmigráfica; ISBN nº 978-989-95946-3-0; Lisboa 2010; pág.40.



Durante as Guerras Peninsulares, o Corpo Telegráfico foi um meio estratégico utilizado pela regência para assegurar a vigilância do território, assim como para Wellington, assumir o controlo efetivo da defesa das Linhas de Torres.

2.2 Guerras Peninsulares

As comunicações telegráficas durante a terceira invasão estavam ao cuidado da armada inglesa que detinha elevado prestígio na área das comunicações.

O telégrafo óptico de bolas utilizado nas linhas de Torres pelas tropas inglesas, permitia transmitir números de quatro algarismos. Os algarismos das dezenas e unidades eram indicados pelo conjunto de bolas penduradas no braço maior. O algarismo das centenas era indicado pelo conjunto de bolas do braço menor e o dos milhares pela apresentação de bolas ou bandeiras na haste vertical.

A Rede Lisboa-Almeida iniciada em 1809 estava concluída quando Massena chegou a esta fortaleza. No entanto, com o recuo das nossas tropas para a Rede de Torres, esta foi abandonada. Só em 1812 a Rede Lisboa -Almeida e as suas ramificações seriam reativadas [20].

Antes da Batalha do Buçaco, Wellington montou uma rede de comunicações de vigilância que incluiu não só as suas próprias comunicações, como também levou à construção de várias outras estações. Estas estações utilizavam os meios da telegrafia portuguesa, e foram dispostas num triângulo definido por Celorico da Beira, Guarda e Almeida. Este sistema poderia garantir a continuidade do serviço, caso algum dos telégrafos ingleses fosse destruído.

Massena acabou por se retirar de Portugal em março de 1811, sendo estas linhas pouco tempo depois desativadas por já não se justificar a sua utilização.

A Rede da Barra e a Rede de Lisboa-Almeida, com ramificações para Elvas e Abrantes, ainda se mantiveram em funcionamento durante mais algum tempo, no entanto, pela impossibilidade de novas invasões, foi perdendo importância e acabou por ser desativada.



Fig. 7 - Recriação do telégrafo de bolas no Buçaco

[20] - LIMA, MGen António Luís Pedroso de; AFONSO, Cor. Aniceto; ALVES MGen Carlos; DIAS, Cor. Jorge Costa; Bicentenário do Corpo Telegráfico 1810-2010; Edição da Comissão Portuguesa de História Militar; Comissão da História das Transmissões; Grafismo: Blueprint, Lda.; Impressão: Palmigráfica; ISBN nº 978-989-95946-3-0; Lisboa 2010; pág.36.



Resumo

Desde a nomeação de Francisco António Ciera como novo Diretor para a Rede da Barra em 1803 a 1810, ano da criação do Corpo Telegráfico, a telegrafia visual terrestre em Portugal teve um grande desenvolvimento.

Para que isto acontecesse, contribuiu grandemente a criação e utilização de um telégrafo mais simples e económico desenvolvido por Ciera. A utilização deste novo equipamento permitiu também, durante a Guerra Peninsular, sobrepor-se com enorme sucesso ao sistema inglês, obtendo assim excelentes resultados. Estes sistemas implementados foram de tal modo inovadores, que só muito mais tarde foram substituídos por novos telégrafos eléctricos.

Os telégrafos utilizados pelo Corpo Telegráfico durante as Guerras Peninsulares, foram essencialmente o de ponteiro e o de palhetas ou persianas. Por parte das tropas francesas foi utilizado o telégrafo de Chappe, sendo o telégrafo de ponteiro utilizado em sobreposição com os sistemas ingleses, sobretudo na eventualidade das tropas inglesas poderem vir a abandonar as suas posições. Estes por seu lado, utilizaram o telégrafo de bolas ou balões, permitindo assim assegurar as comunicações entre a esquadra inglesa ora fundeada no Tejo, ora no Atlântico passando pelas linhas de Torres. Este sistema era no entanto muito dispendioso e difícil de operar, no entanto, quando Massena chegou às Linhas de Torres, o pessoal já estaria bastante treinado.

Bibliografia

SANTOS, General Garcia dos, As Transmissões Militares da Guerra Peninsular ao 25 de Abril. Comissão da História das Transmissões. Autores, PINTO, TGen Pereira, LIMA, MGen Pedroso de, GO-LIAS, TCor Jorge; Coordenação, AFONSO, TCor Aniceto. Colaboração, FALCÃO, Cor. Carlos, DIAS, Cor. Costa, CANAVILHAS, Cor. Lopes; Gráfica: Blueprint Lda.; Impressão Gráfica: Europam Lda. Lisboa, 2008.

LIMA, MGen António Luís Pedroso de, AFONSO, Cor. Aniceto; ALVES, MGen Carlos; DIAS, Cor. Jorge Costa; Bicentenário do Corpo Telegráfico 1810-2010; Edição da Comissão Portuguesa de História Militar; Comissão da História das Transmissões; Grafismo: Blueprint, Lda; Impressão: Palmigráfica; ISBN Nº 978-989-95946-3-0; Lisboa 2010.

LUNA, Isabel de; SOUSA, Ana Catarina; LEAL, Rui Sá; Telegrafia Visual na Guerras Peninsulares. 1807-1814.

FONSECA, Moura da, As comunicações Navais e a TSF na Armada, 1988.

MACEDO, Direção Coronel Tm (Engº) Henrique José da Silva Castanheira, Regimento de Transmissões: 30 Anos de Serviços Distintos 1977-2007; Coordenação RIBEIRO, Tenente-Coronel Tm (Engº) Carlos Jorge de Oliveira; Redação e Edição Estado-Maior do RTm, Batalhão de Comunicações e Sistemas de Informação, Centro de Segurança da Informação; Propriedade: Regimento Transmissões; Impressão M2; 14 Setembro 2007.

VEGAR, José; Vencer a distância - Percorso das Comunicações em Portugal; Museu das Comunicações; Fundação Portuguesa das Comunicações; Design: KAISER, Arne; Impressão: Loures Gráfica. SA.



A COHORT PLC COMPANY

EID é um parceiro na inovação e soberania nacional com soluções C4I desenhadas à medida e com garantia de partilha de informação segura e em tempo real.

Atentos aos desafios atuais e futuros providenciamos soluções completas, de nível superior, de informação no campo de batalha e rápida construção da COP (Common Operational Picture).

Para conhecer melhor todas as nossas soluções, por favor visite-nos em www.eid.pt

Temos uma equipa de especialistas à vossa espera!

TERRANEX
COMUNICAÇÕES TÁTICAS

TECHNOLOGY DRIVEN BY EXPERIENCE





O Exército na edificação de uma capacidade nacional *Federated Mission Networking (FMN)*

Capitão Tm Rui Gomes

Chefe da EqProjSIC-T/DCI

Representante Nacional no FMN CIAV Working Group - Engineering

Introdução

O conceito de *Federated Mission Networking* (FMN) foi desenvolvido em resposta à diretiva do Comité Militar da NATO (MC) de 7 de julho de 2011, exigindo ao *Allied Command Transformation* (ACT), em estreita coordenação com o *Allied Command Operations* (ACO), para desenvolver um conceito genérico e abrangente tendo por base as melhores práticas e lições aprendidas da implementação das Redes de Missão no Afeganistão (*Afghanistan Mission Network* [AMN]).

O objetivo do conceito de Redes de Missão Federadas é fornecer diretrizes de elevada amplitude para a implementação de capacidades relacionadas com os Sistemas de Informação e Comunicações (SIC) e de âmbito Operacional, federadas em *Mission Networks* (MN), que permitam a partilha eficaz de informação entre a NATO, as nações da NATO e parceiras, e/ou Entidades não-NATO, participantes em operações. Uma MN federada deverá ter como princípio a confiança e a determinação, permitindo a ação eficaz de Comando e Controlo (C2) em futuras operações da Aliança e/ou de âmbito multinacional através de uma coligação.

Deste modo, a *Framework FMN* abrange as pessoas, processos e a tecnologia necessária para operar MN federadas, disponibilizando os mecanismos adequados para verificar e validar de forma coletiva a interoperabilidade entre as capacidades dos seus afiliados, permitindo deste modo que os parceiros e afiliados FMN possam partilhar um panorama operacional conjunto e contribuir de forma significativa para o conhecimento situacional, bem como para o planeamento e execução de futuras operações multi-domínio.

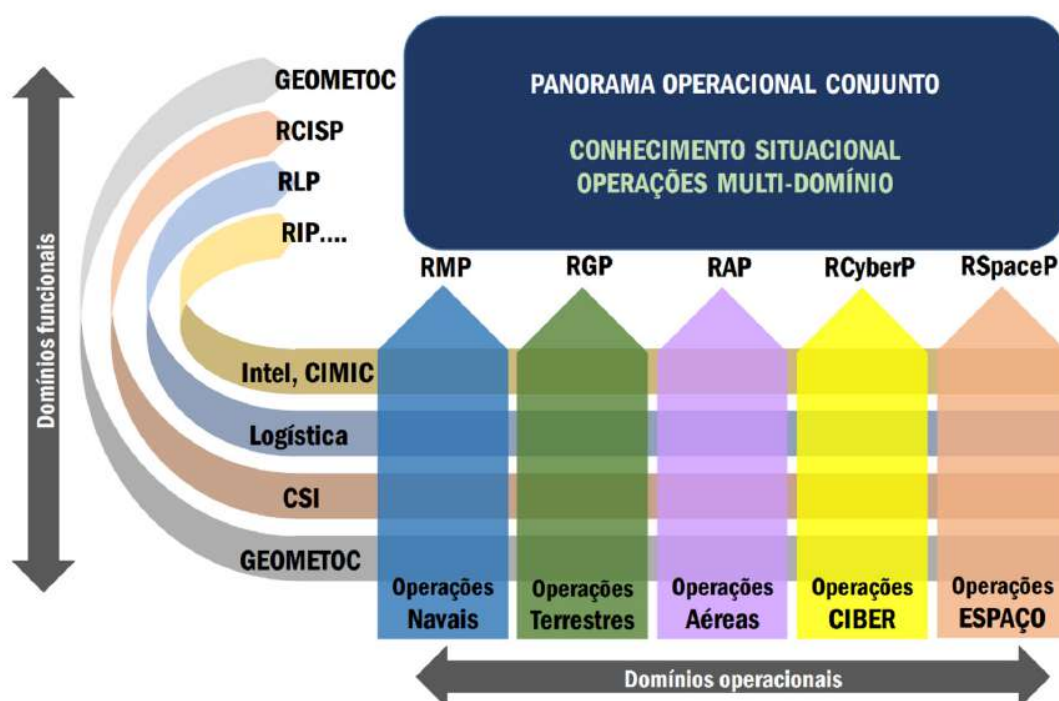


Figura 1 – Paradigma Tecnológico do Comando e Controlo Conjunto



O Processo *FMN Framework* segue uma abordagem em *Spiral* para garantir a continuidade dos resultados e produtos FMN com base em subprocessos persistentes, executados de forma contínua. Desse modo, os produtos e atividades entregues pelo processo da *FMN Framework* são interdependentes e diretamente vinculados à consecução de um ou mais dos objetivos da estrutura FMN, incluindo todos os serviços anteriormente aprovados como objetivos das respectivas *Spirals* precedentes.

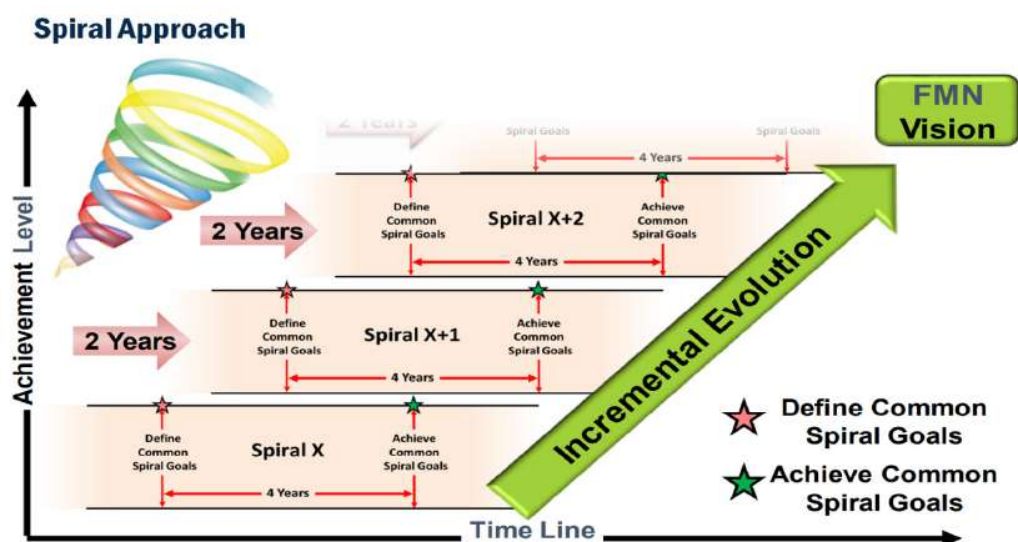


Figura 2 – Desenvolvimento de uma capacidade FMN tendo em conta as várias Spirals

Desenvolvimentos nacionais no âmbito da FMN

No que toca aos compromissos nacionais, a afiliação de Portugal foi aprovada estabelecendo o nível de ambição de Opção B - *Mission Network Extension* (MNX), o que significa que Portugal necessita de ser provedor de alguns serviços, sobretudo os serviços designados como *Core Services*, no entanto tem que ser consumidor para todos.

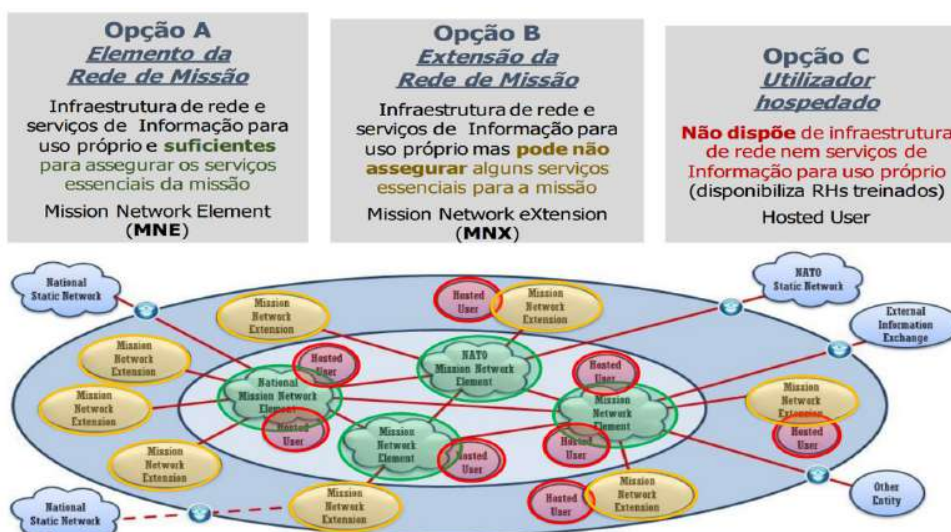


Figura 3 - Organização FMN para a Afiliação



Deste modo, foi assumido também o compromisso de Portugal em participar ativamente nos Grupos de Trabalho e sindicatos, contribuir com um Oficial de Ligação no Secretariado da FMN, desenvolver a Capacidade FMN Nacional e implementar operacionalmente nas forças nacionais.

O plano nacional e o alinhamento estratégico materializado nas propostas efetuadas pelo Estado-Maior das Forças Armadas (EMGFA) pressupõem que é o EMGFA a entidade primariamente responsável pela definição e desenvolvimento da *FMN Framework* a nível nacional, nomeadamente garantir a participação nacional nos diversos grupos de trabalho internacionais da FMN, sendo que o planeamento de capacidades e coordenação operacional, projetos, controlos de configuração e edificação e capacitação de Forças deverá ser responsabilidade dos Ramos.

Este aspeto é relevante, sobretudo tendo em conta que o Exército assumiu um conjunto de *Targets* perante a União Europeia e com a NATO, prevendo por isso a breve trecho participar em operações conjuntas e combinadas que exigem a implementação de MN federadas com base no conceito FMN, como é o caso do *European Union Battle Group 2025/2026* (EUBG-25/26), ou a participação na Força Nacional Destacada (FND) da Roménia, devendo por isso ter em consideração os requisitos mínimos para a implementação de capacidades SIC projetáveis definidos pela NATO, tanto para o nível operacional como para o nível tático.

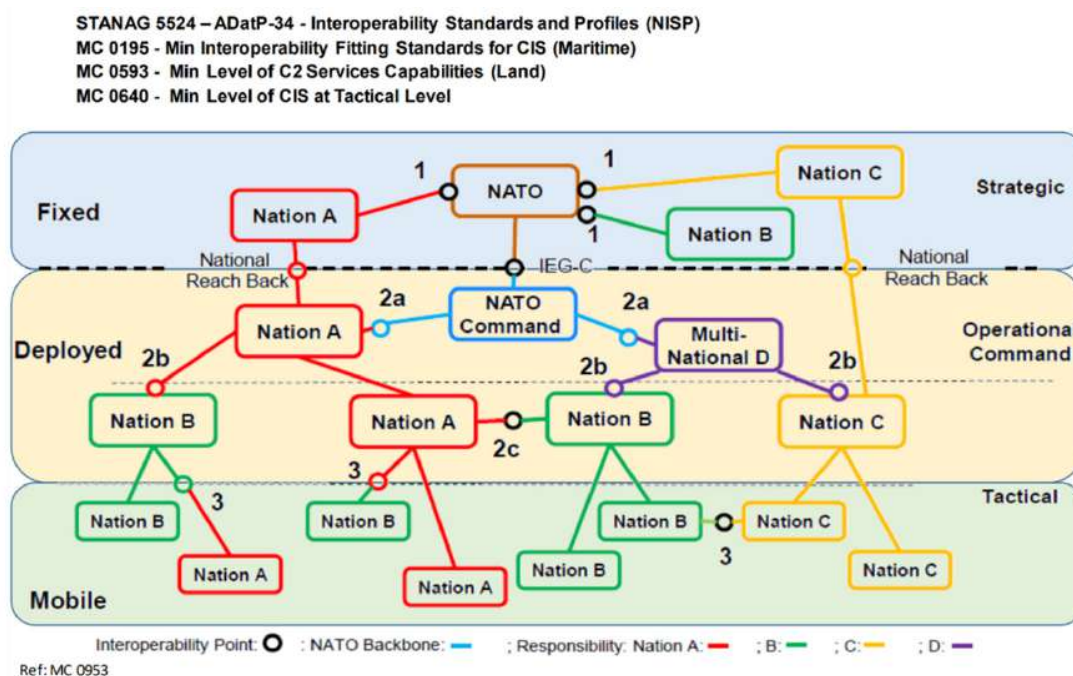


Figura 4 – Standards de Interoperabilidade

Portugal assumiu a participação em vários eventos de *Assurance, Verification and Validation* (AV&V) para os *Core Services*, tendo utilizado a série de exercícios CWIX para validar e confirmar as suas capacidades conjuntas, sendo de realçar que em 2023 foi finalizada a validação formal de diversos serviços *FMN Spiral 3*, sobretudo vários *Core Services* e *Friendly Force Tracking*.



Figura 5 - Participação de Portugal no exercício CWIX (esquerda) e V2CN (direita)

Está previsto que em 2024 seja realizada a validação formal de um conjunto alargado de *Core Services*, através da participação de Portugal no exercício *Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise* (CWIX) 2024, e pela primeira vez num evento de validação de *Request for Change* (RFC) que será realizado na rede de laboratórios federados *Combined Federated Battle Laboratories Network* (CFBLNet), sendo fundamental o apoio de planeamento e coordenação efetuado pelos representantes nacionais do FMN Coalition Interoperability Assurance and Validation Working Group (CIAVWG).

Em paralelo, desde 2018 que uma equipa conjunta se desloca a Madrid para participar no exercício espanhol *Validación, Verificación y Confirmación Nacional* (V2CN) onde são efetuados testes de validação e verificação com as capacidades FMN espanholas, permitindo a instanciação de uma rede de missão de acordo com o cenário aprovado entre os dois países, alinhando estratégias e requisitos operacionais de interoperabilidade.

Todas estas participações, na vertente dos *Core Services*, foram garantidas com verbas previstas pelo EMGFA para o programa FMN nacional, tendo participado várias equipas conjuntas multidisciplinares compostas por militares do EMGFA e dos Ramos.

Seguidamente são apresentados os serviços que Portugal necessita de implementar, ao longo das várias *Spirals*, bem como uma indicação temporal da duração possível dos trabalhos de atualização contínua da *Baseline* Nacional.

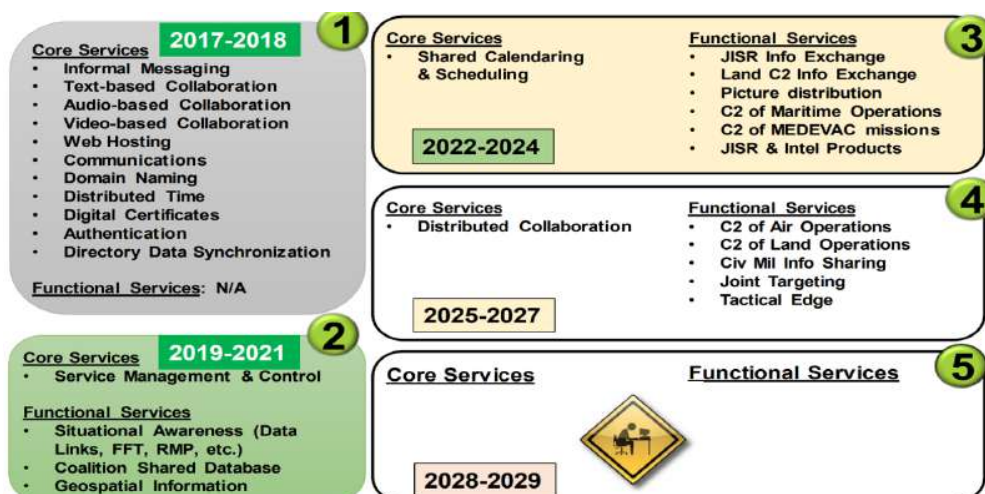


Figura 6 - Serviços Core e Funcionais previstos em várias *Spirals* do FMN (incrementando sempre aos serviços já existentes nas Spirals anteriores)



No último ano 2023 verificou-se um elevado desenvolvimento a nível procedimental e técnico, sobretudo no âmbito da participação de Portugal no grupo de trabalho CIAVWG, muito graças à boa vontade, esforço e dedicação dos elementos que constituem este grupo dos vários Ramos, o que permitiu edificar um laboratório FMN na rede de laboratórios federados, nomeadamente através do acesso à rede CFBLNet.

Em novembro de 2023, elementos do CIAVWG, apoiados por outros elementos dos Ramos e do EMGFA, participaram pela primeira vez num *Joining Event*, tendo implementado, federado e obtido 100% de sucesso nos *Test Cases* realizados. Foram apenas implementados os *Core Services* mandatórios para que fosse possível integrar a comunidade FMN nesta rede federada, nomeadamente *Text-based Collaboration, Communications, Domain Naming, Distributed Time e Digital Certificates*, sendo que neste momento o próximo objetivo será iniciar a implementação de serviços funcionais e de sistemas de C2.

O planeamento, organização e participação nestes eventos de validação exigem em antecipação um elevado empenhamento, sobretudo dos grupos FMN CIAVWG e *Change and Implementation Coordination Working Group* (CICWG), que culmina no processo de validação formal e execução de testes técnicas da implementação de todos os serviços e produtos, que tem que ser repetido sempre que existe um novo produto que se pretenda inserir na *Baseline* Nacional ou sempre que inicia o processo de validação de capacidades para uma nova *Spiral*.

Edificação de capacidades FMN no Exército

No que toca à edificação de capacidades FMN no Exército, o único projeto que realmente contribui para este âmbito de forma significativa é o projeto *Tactical Deployable Communications and Information System* (TDCIS), conduzido em parceria com a *NATO Communications and Information Agency* (NCIA), estando previsto o seu início no presente ano de 2024, já com o contrato assinado no primeiro trimestre do presente ano de cerca de 33,2 M€.

Este projeto TDCIS materializa-se no projeto Sistema de Informação e Comunicações – Tático (SIC-T) desenvolvido pelo Exército, embora com alterações significativas na arquitetura inicial do sistema, com vista a incluir devidamente especificações que garantem que todos os módulos entregues ao Exército serão FMN *compliant* com a *Spiral* 3, e posteriores.

Seguidamente serão apresentadas algumas arquiteturas de alto nível que serão implementadas nos novos módulos SIC-T e que estão devidamente alinhadas com os normativos FMN.

De uma forma geral, o projeto TDCIS continua adequado aos requisitos operacionais definidos para o projeto SIC-T, no entanto a implementação do novo projeto e operacionalização do mesmo exigirá seguramente diversas atualizações, quer seja ao nível procedimental e técnico das operações CSI a nível nacional, quer seja ao nível da doutrina do Exército, que ocorrerão seguramente a seu tempo logo que oportuno.



Uma das alterações mais significativas está relacionada com os diferentes domínios de segurança que serão implementados nos novos módulos, nomeadamente as seguintes Colored Clouds (CC):

- **UNCLASSIFIED (xU)** - poderá interligar com a Rede de Dados do Exército, ou qualquer outra rede de âmbito não classificado;

- **RESTRICTED (xR)** – Domínio que será utilizado em todas as operação que necessitem de implementar serviços de *Tactical Edge Communications*.

Neste domínio serão integrados os Rádio Tácticos de Combate dos módulos e dos utilizadores móveis, bem como os sistemas de C2 de nível tático, tais como o *Battlefield Management System*, o sistema *Dis-mounted Soldier System* – C2, ou quaisquer outro de interesse, tais como *Android Team Awareness Kit* (ATAK), *Windows Team Awareness Kit* (WinTAK), etc;

- **SECRET (xS)** - Neste domínio serão implementados todos os serviços de acordo com as especificações FMN e será a rede de missão utilizada primariamente para federação com outros afiliados FMN e/ou outras capacidades FMN nacionais desenvolvidas pelo EMGFA e pelos Ramos.

Todos os novos módulos SIC-T implementam a capacidade *Protected Core Networking* (PCN), de acordo com o STANAG 5637, nomeadamente as interfaces PCN-1 e PCN-2, bem como as funcionalidades de *E-Node* e *P-Function*, existindo, portanto, um domínio adicional para este efeito designado por **BLACK**, no qual se ligam todos os sistemas de transmissão pretendidos (e.g. *mini- Line of Sight* (LOS), LOS, *Satellite Communications* (SATCOM), *Mobile 4G/5G*, *High-Capacity Data Radio* (HCDR), meios filares, entre outros).

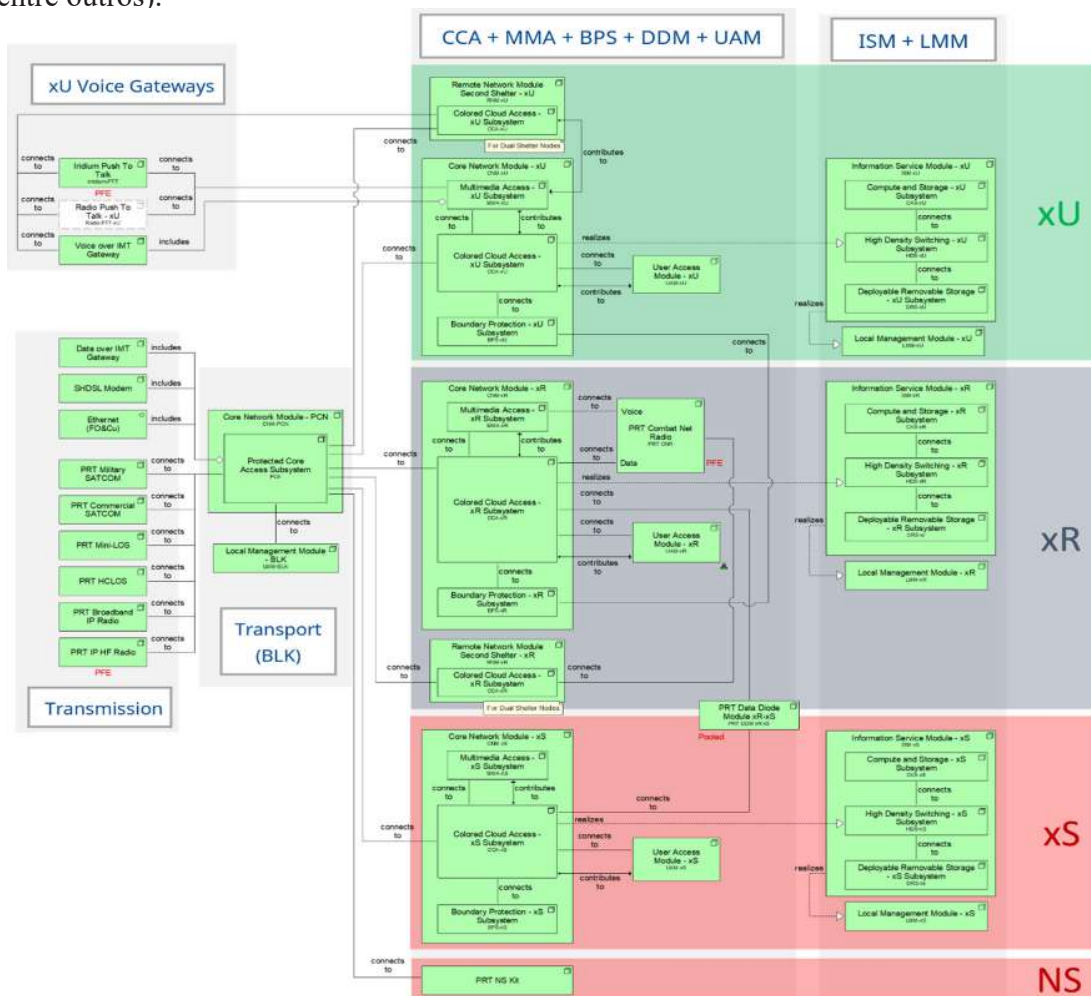


Figura 7 – Arquitetura Genérica dos novos Módulos SIC-T (alterações em alguns dos submódulos existentes consoante a tipologia de módulo SIC-T)



No que toca à capacidade de garantir interoperabilidade com outras forças, os módulos *Access Node* (NA), *Battalion Communications Center* (BCC) e *Company Communications Center* (CCC) são aqueles em que está prevista a capacidade para implementação de serviços e a possibilidade de se federarem com outros parceiros afiliados FMN.

Foi definido que os módulos de tipologia BCC deveriam ter essa capacidade pronta, tendo em conta as ambições e os compromissos internacionais em que o Exército participa.

Foi também solicitado que o módulo CCC tivesse essa capacidade como *Enabled*, na eventualidade de ser necessário efetuar esta integração utilizando um módulo desta tipologia, bastando que seja reforçado para o efeito com equipamentos/sistemas adicionais no domínio xS, que por norma não faz parte do módulo CCC, no entanto poderá ser facilmente adicionado nos novos módulos.

Deste modo, foi previsto o desenvolvimento de um ponto de interoperabilidade, a ser disponibilizado pelos módulos, designado por *Interconnection to Nations*, cujo conceito de implementação é de acordo com a figura seguinte:

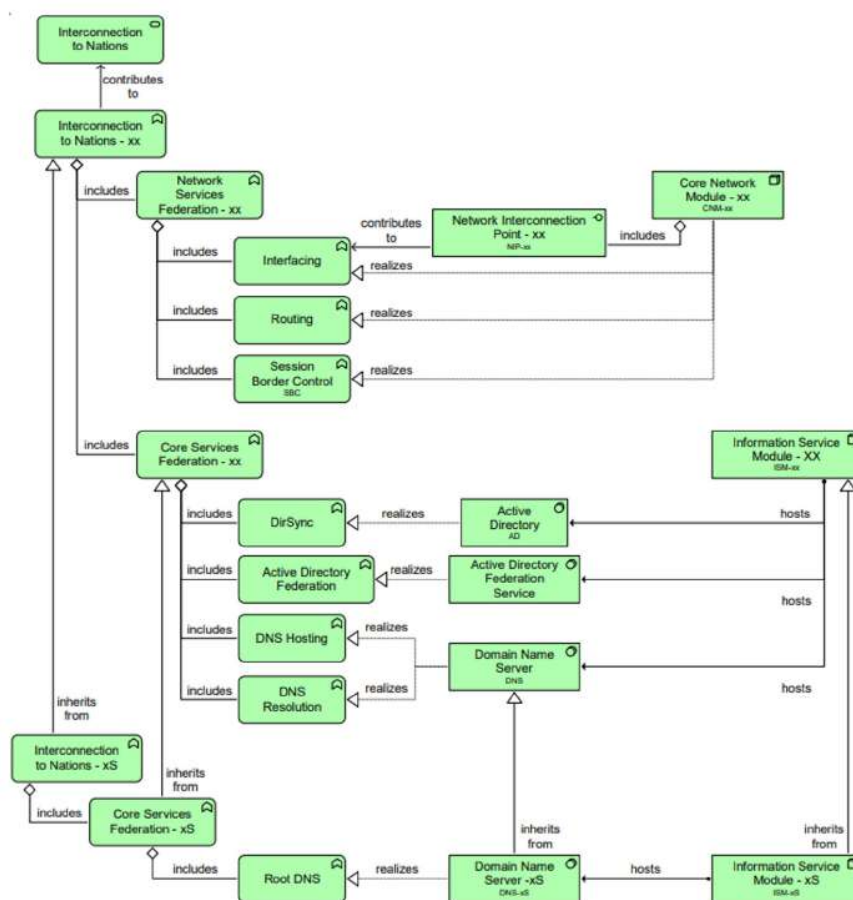


Figura 8 – Arquitetura do serviço *Interconnection to Nations* dos novos módulos SIC-T



Deste modo, o serviço de Interconnection to Nations depende dos seguintes elementos (pelo menos):

- Do *Core Network Module* (CNM):
 - o A interface *Network Interface Point* (NIP) que interliga os Mission Partners de forma física e lógica;
 - o Funções de roteamento para federar ao nível da camada de rede;
 - o Funções de *Session Border Control* (SBC) para federar serviços colaborativos de comunicações (Audio&Video) .
- Do *Information Service Module* (ISM):
 - o O *Active Directory* (AD) para sincronização de diretórios e para permitir federação e estabelecimento de relações de confiança entre domínios;
 - o *Software* de Email para federar o serviço de *Informal Messaging*;
 - o *Domain Name Server* (DNS) para permitir efetuar *DNS hosting* e Resolver para a federação. Neste caso, este *DNS Server* a operar no domínio xS deverá permitir a implementação de *Root DNS*.

O projeto TDCIS prevê também a aquisição de um NATO SECRET (NS) Kit, que não sendo um domínio presente em todos os módulos SIC-T, poderá facilmente utilizar a sua infraestrutura de transporte para aceder à informação existente na *NATO Secret Wide Area Network* (NSWAN).

Por fim, em termos conceptuais, a interligação entre qualquer tipo de módulo SIC-T será realizada de forma substancialmente diferente daquela a que normalmente os seus administradores e operadores estão habituados aos dias de hoje.

As implementações atuais, a doutrina e os procedimentos estão ainda longe de estarem devidamente alinhadas com as normas FMN, que são na verdade aquelas que o Exército deverá implementar a breve trecho nas suas FND em que participe em operações de âmbito FMN, i.e. União Europeia e NATO. Seguidamente é apresentado um esquema com as ligações previstas entre dois módulos SIC-T no âmbito do projeto, utilizando sempre a PCN como meio de transporte para interligação das diversas CC, cada uma delas correspondendo a um determinado tipo de domínio de segurança.

Deste modo, também será necessário de futuro que a interligação com as redes administrativas de carácter Não Classificado (e.g. Rede de Dados do Exército) seja realizada de forma adequada com base nos standards FMN e na arquitetura revista dos módulos SIC-T, com vista a treinar procedimentos, configurações, técnicas e aprofundar conhecimento e experiência, procurando treinar em casa os cenários que se podem encontrar em ambiente internacional.

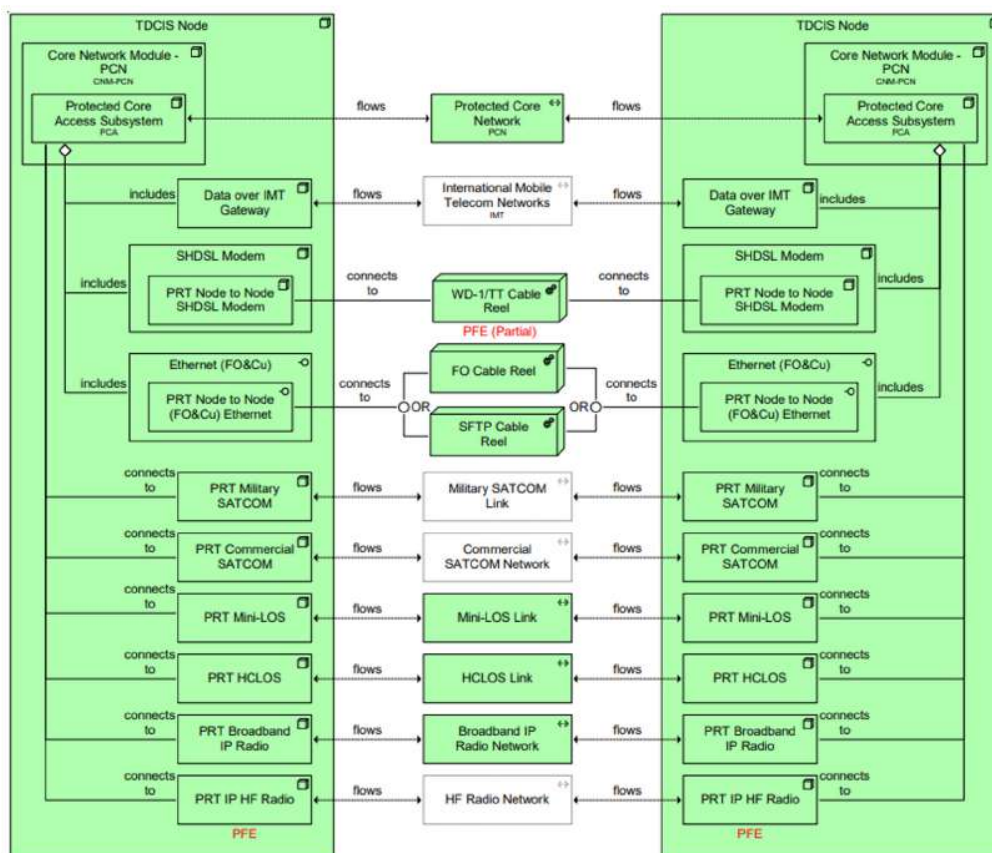


Figura 9 – Possibilidades de interligação entre dois módulos SIC-T, de acordo com a implementação da PCN e dos normativos FMN

Conclusões

Nesta fase, prevê-se que na melhor das hipóteses a entrega dos primeiros módulos SIC-T possa ser realizada em final de 2025, início de 2026, sendo que o presente ano de 2024 será um ano relevante, na medida em que será realizado o *Low Level Design* dos módulos de comunicações, juntamente com a empresa vencedora do concurso internacional e com a NCIA, contando com a participação intensiva do Grupo e Equipa de Projeto SIC-T nestes trabalhos técnicos.

Como tal, na melhor das hipóteses, a partir de 2025 o Exército poderá iniciar os processos necessários para a validação formal dos seus novos módulos, no âmbito da participação nos diversos Grupos de Trabalho FMN em que está envolvido, com vista a acelerar a inclusão das novas capacidades e sistemas na *Baseline* FMN Nacional, a partir da *FMN Spiral 4* e posteriores.

Para o efeito, a modernização das infraestruturas que irão acomodar os módulos SIC-T, bem como a construção de espaços laboratoriais com acesso à rede *CFBLNet*, nomeadamente no Regimento de Transmissões, permitirão disponibilizar formação e treino adequado aos administradores de sistemas e operadores dos módulos, sendo por isto esta atividade de carácter absolutamente fundamental, pois só assim o Exército garantirá que os seus militares de Transmissões podem ser devidamente preparados para os complexos desafios futuros.



Sendo o Exército um dos principais Ramos interessados em investir nas capacidades FMN, tendo em conta a natureza das suas operações e por ser até à data o único Ramo a investir em capacidades FMN projetáveis, urge que seja merecida a atenção necessária em torno da edificação destas capacidades.

Por outro lado, devem ser feitos esforços no Exército no sentido de se acompanhar a evolução tecnológica que a *Framework FMN* impõe ao seus Afiliados, permitindo ainda canais flexíveis e ágeis para que o conhecimento adquirido até agora sobre o conceito FMN seja disseminado internamente na instituição, através da criação de estruturas e de processos robustos e adequados, a fim de permitir que os representantes do Exército nos grupos de trabalho FMN tenham condições para cumprir as suas missões e apoiar na melhoria dos sistemas nacionais, colaborando para que Portugal e o Exército cumpram formalmente com os compromissos internacionais, bem como para que os futuros administradores e operadores desta capacidade sejam devidamente enquadrados, treinados e preparados para os futuros desafios que possam surgir nos próximos tempos.





Exercício GOLFINHO 23

Capitão Tm João Félix
Técnico de Sistemas na EP SIC-T

A Direção de Comunicações e Informação através da sua Equipa de Apoio em Engenharia do Projeto Sistema de Informação e Comunicações – Tático (EP SIC-T) participou no exercício Golfinho 23 que decorreu na Zona Militar da Madeira, ZMM.

Numa situação de catástrofe ou acidente grave, pode ser necessário o apoio do Exército no âmbito do Apoio Militar de Emergência, assim como no apoio de tarefas e ações no âmbito da proteção civil. Este exercício teve como finalidade testar a capacidade do Comando da ZMM na vertente de Comando e Controlo (C2) no apoio de uma operação de resposta a catástrofe.

O objetivo principal das Transmissões neste exercício, foi demonstrar as reais capacidades dos seus equipamentos e sistemas em apoio de C2, nos vários cenários de catástrofe criados no decorrer do Exercício GOLFINHO 23, validando assim o conceito desenvolvido para a implementação do projeto da Lei de Programação Militar (LPM) “Defesa Imediata dos Arquipélagos”.

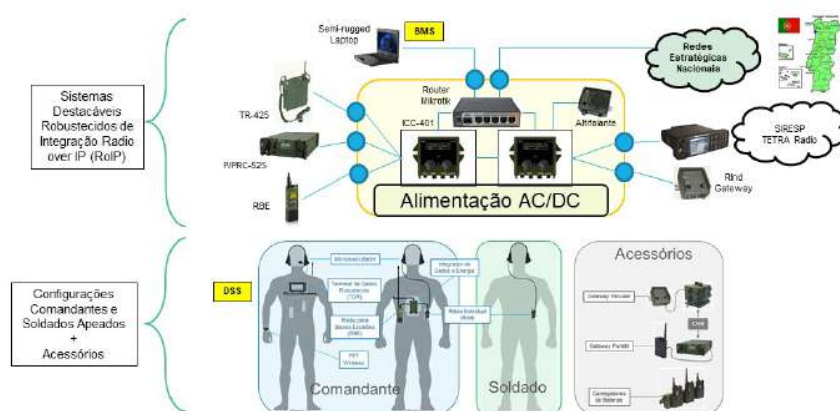


Figura 1 – Arquitetura Rede - Defesa Imediata dos Arquipélagos

O sistema da figura 1 é composto pelo ICC-401, da empresa EID, onde são ligados os equipamentos rádio, podendo estes ser analógicos ou digitais. Este intercomunicador foi conectado a um *router/switch* que permite o acesso dos vários componentes dos sistemas de C2 aos rádios, assim como permite o acesso das várias tipologias de redes rádio intervenientes, interligando a componente operacional e tática, estendendo a capacidade de ambas. Este projeto prevê a aquisição de meios idênticos aos do projeto de sistemas de combate do soldado (SCS), da componente C4I. Os meios rádios são o HR5000 (Rádio de Baixos Escalões - RBE) e o TWH 104 (Rádio Individual - RInd).

O Exército possui uma grande quantidade de equipamentos rádio da família PRC-425, com tecnologia da década de 80 do século passado, na ZMM. É principalmente com recurso a este tipo de rádio, que a ZMM desenvolve as suas ações e garante a capacidade de comunicações das suas forças para as missões que lhes estão atribuídas. De forma a rentabilizar os meios existentes foi desenhada uma solução que permite a interoperabilidade em fonia desta família de rádios analógicos com o RInd, RBE e P/PRC-525 (em modo seguro) rádios utilizados pelo Exército e que têm a capacidade de transmissão de dados em modo seguro.



Foi também integrado no ICC-401 o rádio Sepura SRG3900, utilizado pela SIRESP para a sua rede TETRA, interligando assim as capacidades da Proteção Civil com as capacidades que o Exército dispôs no terreno.

Os meios adquiridos no âmbito das aquisições para a capacidade do SCS permitem formar equipas. Estas equipas trabalham com uma topologia onde está presente um chefe de equipa equipado com Terminais de Dados Robustecidos (TDR), que tem instalado o *Dismounted Soldier System* (DSS), que é o software de C2 para baixos escalões em implementação no Exército. Com recurso a estes meios, os seus utilizadores conseguem visualizar em tempo real as posições dos elementos da sua equipa, assim como os elementos das várias equipas que estiverem em operações naquele cenário. Com estes sistemas, o Exército consegue apoiar com militares projetados no terreno, mantendo uma Situational Awareness dos seus meios humanos assim como partilhar esta informação com as várias entidades intervenientes, ou que necessitam de ter acesso a esta informação.

Num mundo cada vez mais digital, a capacidade de fonia continua a ser um elemento primário e fundamental neste tipo de apoios. A possibilidade de interligar os vários tipos e tecnologias de meios rádio das entidades que concorrem para prestar apoio em situação de catástrofe, permitindo a integração de voz entre todas elas, com o acréscimo de ter disponível uma Situational Awareness através de visualização dos meios no terreno em sistema de C2, é uma mais valia essencial em apoios desta natureza.



Figura 2 – Zonas de sombra SIRESP na ZMM

A ZMM tem algumas zonas sombra onde não existe cobertura de rede SIRESP, nem outro tipo de comunicações alternativas. Neste exercício foram simulados vários incidentes onde foi necessário o emprego da solução em cima descrita, de modo a estender a capacidade de comunicações até ao local onde era necessário.



Como exemplo, na Ponta de São Lourenço não é possível comunicar para o Regimento de Guarnição nº3 (RG3) ou para a Unidade de Apoio da ZMM (UnAp/ZMM). Neste cenário, foi simulado um incidente neste local, Ponta de São Lourenço, onde, como já descrito, não existe cobertura de rede. Neste caso foi instalada uma Shelter com os meios integradores e várias redes rádio, num local com bom acesso a comunicações Militares e SIRESP, que fez a ponte entre as equipas que executaram as operações de resgate (simuladas), que possuíam meios de comunicações e C2. Foi possível às entidades seguirem em tempo real a condução das tarefas necessárias durante a execução do resgate. No Centro de Operações Terrestres, instalado na UnAp/ZMM, assim como no RG3, foi possível visualizar o desenrolar de todos os acontecimentos através do *Battefeld Management System* (BMS), que recebia os dados do DSS das equipas, ao mesmo tempo que ouviam todas as comunicações efetuadas por fonia, utilizando os meios rádios ao dispor.

Conforme se pode ver na figura em baixo, foi utilizado um dos repetidores existentes da família do PRC-425 instalado na ZMM, no Pico do Areeiro.



Figura 3 – Locais utilizados no exercício

O centro de operações foi operacionalizado na UnAp/ZMM e foi instalado na shelter a solução integradora e os diversos rádios/antenas, na posição graficada na figura 3; Ligou-se um checkpoint com dados móveis (simulação de um terminal satélite), que permitiu a injeção de dados na Rede de Dados do Exército (RDE). Instalou-se um terminal com o BMS que permitiu a integração dos dados (posições GPS, mensagens, CHAT, etc.) com o BMS que se encontrava no Posto de Comando;

O RG3 teve acesso às comunicações voz via PRC-525 e/ou PRC-425, pois foram utilizadas comunicações em frequência fixa, devido ao repetidor utilizado. A UnAp acedeu às comunicações via rádio e dispunha de um computador com o BMS. Esta solução possibilitou o acesso das posições dos militares que se encontravam a prestar apoio na Ponta de São Lourenço. Todas as comunicações militares estavam integradas na rede SIRESP.



Figura 4- Visualização do BMS com a common operational picture (COP)

No decorrer do Exercício Golfinho23 existiram outros incidentes, onde havia “linha de vista” do ponto de vista rádio para o PC, ou seja, as comunicações eram diretas sem recurso a repetidor. Neste caso a voz e os dados eram partilhados via meios rádio (PRC-525 e/ou RBE).

Concluindo: este sistema vai permitir integrar comunicações militares dos meios já existentes no Exército, assim como de meios em aquisição, com outros sistemas de comando, controlo e coordenação de comunicações para emergências e segurança, nomeadamente, da rede rádio do Sistema Integrado de Redes de Emergência e Segurança de Portugal (SIRESP), assim como da Rede Integrada de Telecomunicações de Emergência dos Açores (RITERAA), ou outras, assumindo-se como uma solução de comunicações de muita flexibilidade e com potencial emprego em operações e tarefas de natureza variada.



Figura 5- Interior da Shelter



A estruturação de um SOC – diferenças entre os SOC empresariais e o GOC do Exército

Capitão Tm Helder Reia

Chefe no Núcleo de Monitorização e Análise/ GOC/ CGIC

1. Enquadramento

Face ao aumento de ameaças no espectro cibernético, tanto na quantidade de malwares e softwares potencialmente perigosos como nas ameaças de rede emergentes, as empresas e instituições a nível mundial estão obrigadas a reforçar as suas equipas de segurança. Nos últimos anos, a incidência de ciberataques tem crescido exponencialmente em todo o mundo, refletindo a complexidade e sofisticação em constante evolução das ameaças digitais. De acordo com o Relatório de Ameaças à Segurança na Internet (ISTR) da *Symantec*, em 2022, o número de ameaças cibernéticas aumentou em 64%, atingindo níveis alarmantes. Portugal, como parte integrante deste cenário global, não permanece imune a esta tendência.

Em território nacional, dados do Centro Nacional de Cibersegurança (CNCS) indicam que, em média, são detetados mais de 100 incidentes de segurança por dia, variando desde ataques de phishing a intrusões mais sofisticadas. Este aumento notável de incidentes ressalta a urgência de reforçar as medidas de cibersegurança em todas as frentes.

Adicionalmente, o Relatório Anual de Cibersegurança da União Europeia destaca a importância de uma abordagem coordenada entre os estados-membros para enfrentar ameaças cibernéticas transfronteiriças. Este cenário reforça a necessidade de investir em infraestruturas de cibersegurança avançadas, criando os *Security Operations Centers* (SOC).

2. Estrutura de um SOC

Para enfrentar o aumento das ameaças descritos anteriormente, a criação de um SOC surge como uma resposta eficaz. Um SOC é um centro de comando e controlo especializado na monitorização, deteção, resposta e mitigação de ameaças cibernéticas. Na Figura 1 podemos ver todas as funções que um SOC idealmente deve conter, bem como as tarefas a executar para cada função. De forma mais simplificada, um SOC deve ser dividido em camadas, criando uma hierarquia, com as seguintes funções:

- *Tier 1* – Analista Júnior – responsáveis pela análise primária aos incidentes, efetuando a triagem do que é ou não um incidente, diferenciando ofensas reais de falsos-positivos. Este analista deve ainda, com uma maior maturidade na área, identificar eventos de segurança de alto risco, que podem levar a futuros incidentes. Caso este analista não consiga resolver um incidente, este deve escalar o mesmo para um Analista Sénior ou um Elemento de Resposta a Incidentes.

- *Tier 2* – Resposta a Incidentes – analistas que visam a responder aos casos escalados pelos analistas de *Tier 1*, efetuando uma análise mais profunda, seguindo o caminho de um possível ataque e identificando possíveis máquinas infetadas na rede. Quanto mais detalhado e preciso o trabalho realizado pelo analista de *Tier 1*, mais rápida será a resposta ao incidente. Um elemento de resposta a incidentes deve também efetuar relatórios sobre os incidentes e comprometimentos, bem como estudar e implementar medidas de mitigação aos mesmos.



• Tier 3 – *Threat Hunting* – pessoal mais experiente integrante de um SOC, responsáveis por auxiliar em incidentes de larga escala, quando os elementos de *Tier 2* não conseguem efetuar uma resposta em tempo útil. Além disso, realizam e supervisionam análises de vulnerabilidade e testes de penetração para identificar possíveis vetores de ataque. A sua responsabilidade mais importante é identificar proativamente ameaças, lacunas de segurança e vulnerabilidades que possam ser desconhecidas. Devem também recomendar formas de otimizar as ferramentas de monitorização de segurança implementadas à medida que adquirem conhecimento substancial sobre uma possível ameaça aos sistemas.

• Gestor de um SOC - Os gestores de SOC supervisionam a equipa de operações de segurança. Fornecem orientação técnica, se necessário, e são responsáveis por gerir adequadamente a equipa. Isso inclui recrutamento, formação e avaliação dos membros da equipa, criação de processos, análise de relatórios de incidentes e desenvolvimento e implementação de planos de gestão de incidentes necessários. Também supervisionam os aspetos financeiros de um SOC, apoiam auditorias de segurança e prestam contas ao diretor de segurança da informação (CISO) ou a uma posição de gestão de nível superior correspondente.

Para uma instituição da dimensão do Exército Português, com cerca de 5000 utilizadores a apoiar, um SOC deve conter, no mínimo 5 Analistas de *Tier 1*, 2 Elementos de Resposta a Incidentes, 2 *Threat Hunters* e 1 Gestor de SOC, todos a trabalharem única e exclusivamente nas suas tarefas previamente identificadas.

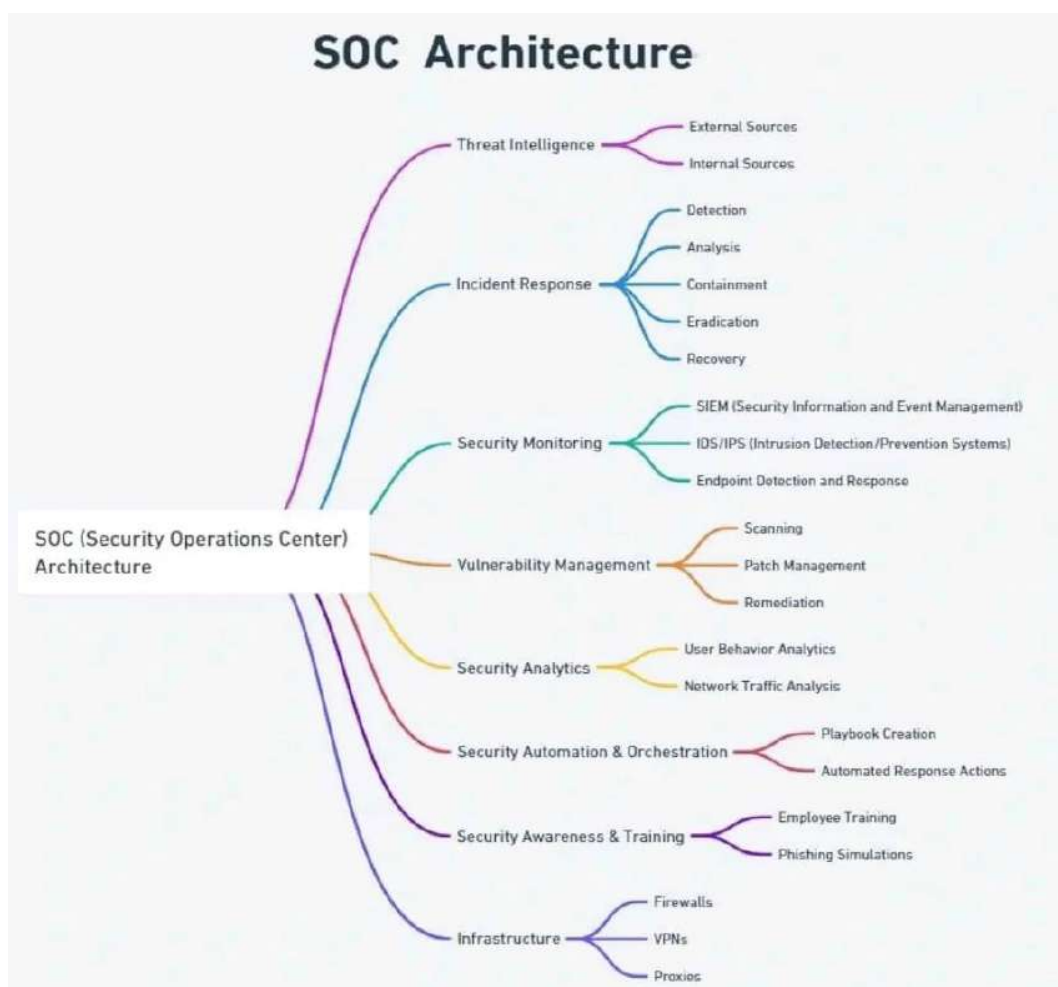


Figura 1 – Arquitetura completa de um SOC



Para além da quantidade a ser garantida, a qualidade dos elementos de um SOC deve também ser tida em conta. Como tal devem ser considerados os anos de experiência e a formação obtida ou a obter por cada função. Para cada camada, os elementos devem ter o tempo de experiência adequado e alguns cursos como por exemplo:

- Analista *Tier 1*:

- o 1 a 2 anos de experiência em funções de suporte de segurança, análise de logs ou administração de sistemas;

- o Formações: Certificação *CompTIA Security+*, Certificação *EC-Council Certified Security Analyst (ECSA)*, *Cisco Certified CyberOps Associate*. Outras formações em sistemas e redes considera-se também útil para o desempenho da função e mais rápida progressão.

- Elemento de Resposta a Incidentes *Tier 2*:

- o 3 a 5 anos de experiência como Analista de *Tier 1* e com experiência em relatórios e gestão de crises no ciberespaço.

- o Formação: Certificação *GIAC Certified Incident Handler (GCIH)*, Certificação *EC-Council Certified Incident Handler (ECIH)*, Cursos *SANS SEC504 (Hacker Tools, Techniques, Exploits, and Incident Handling)* e *SEC599 (Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses)*.

- Elemento de *Threat Hunting Tier 3*:

- o Pelo menos 5 anos de experiência em deteção proativa de ameaças e análise comportamental.

- o Formação: Certificação *Certified Threat Intelligence Analyst (CTIA)*, Certificação *EC-Council Certified Threat Intelligence Analyst (CTIA)*, Cursos *SANS SEC511 (Continuous Monitoring and Security Operations)* e *SEC564 (Red Team Operations and Threat Emulation)*.

- Gestor de SOC:

- o Pelo menos 8 anos de experiência em cibersegurança e em gestão de equipas.

- o Formação: Certificação *Certified Information Systems Security Professional (CISSP)*, Certificação *Certified Information Security Manager (CISM)*, Cursos *SANS MGT512 (Security Leadership Essentials for Managers)* e *MGT514 (Security Strategic Planning, Policy, and Leadership)*.

3. Grupo de Operações no Ciberespaço

Paralelo ao exposto no ponto anterior, existem, dentro das várias competências do Centro de Guerra de Informação e Ciberespaço (CGIC), as competências de executar e coordenar a segurança da informação, das operações em redes de computadores, da ciberdefesa, de comando e controlo e das operações de informação e de garantir a capacidade de resposta do Exército face à ocorrência de incidentes de segurança, assegurando a defesa do ciberespaço e da sua informação.

Para executar estas tarefas, foi criado, dentro deste Centro, o Grupo de Operações no Ciberespaço, sendo este a materialização de um SOC, com algumas diferenças da estruturação referenciada anteriormente. Este grupo, contém na sua orgânica, o seu Comando, o Núcleo de Monitorização e Análise, o Núcleo de Resposta a Incidentes, o Núcleo de Proteção Periférica e uma Secção de Exploração.



Por comparação às várias camadas referenciadas no Ponto 2., o Núcleo de Monitorização e Análise contempla as tarefas dos Analistas de *Tier 1*, o Núcleo de Resposta a Incidentes contempla as tarefas dos Elementos de *Tier 2*, a Secção de Exploração contempla algumas tarefas dos Elementos de *Threat Hunting* (*Tier 3*) e o Comando do Grupo visa a efetuar as tarefas de Gestor do SOC.

Na comunidade de ciberdefesa existem duas linhas de pensamento, uma em que a Proteção de Perímetro, com as tarefas de gestão de firewalls, das políticas de acesso à internet e aos terminais de VPN, deve pertencer ao *Security Operation Center*, enquanto que outra defende que esta componente deve estar no *Network Operations Center* – Centro onde são geridas as redes e serviços. No Exército Português, esta componente está presente no Grupo de Operações no Ciberespaço, facilitando assim a visibilidade dos acessos à internet e os bloqueios de ataques externos.

4. Criação e constituição de uma CIRT e do Núcleo CIRC

Para além da estruturação de um SOC/GOC, devem ser criadas equipas para a resposta aos incidentes que relevem ter uma maior urgência, por forma a responderem a incidentes que envolvam o deslocamento a qualquer área geográfica onde ocorreu o incidente.

Como tal, deve ser criada uma equipa especializada, essencial para garantir uma resposta rápida e eficaz a ameaças emergentes. Esta equipa desempenha um papel crítico na contenção e mitigação de incidentes. As suas tarefas são semelhantes às das diversas funções, com especial ênfase na análise forense e na resposta aos incidentes.

Por norma, estas equipas trabalham em turnos que permite abrangência total pelas 24 horas do dia. Isto, pode ser garantido de duas maneiras, garantindo uma escala de 24 horas, cobrindo principalmente as horas fora do horário laboral ou, em alternativa, funcionando num horário de rotatividade horária, em três turnos de 8 horas.

De forma a garantir uma equipa de resposta não só no Exército como também nas Forças Armadas, foi levantado organicamente o Núcleo CIRC do Exército. Este Núcleo é levantado por militares do Grupo de Operações no Ciberespaço, ficando sob a responsabilidade do Comando de Operações de Ciberdefesa (COCiber). Constituintes deste Núcleo, estão também os CIRC dos restantes Ramos, bem como o CNCS. O Núcleo CIRC responde perante o NCIRC, conforme podemos verificar na Figura 2, podendo ser solicitado pelo mesmo.



Figura 2 - Estrutura dos CIRC a nível das Forças Armadas

5. Conclusões

Neste artigo é possível verificar algumas diferenças entre a constituição de um SOC Civil e o GOC militar. Contudo, apesar das diferenças, é verificável que os processos e orgânica do GOC é compatível com a orgânica constituída no mundo civil.

É necessário, contudo, estabelecer procedimentos mais incisivos, não só a nível da ciberdefesa, como a nível dos sistemas e redes no Exército Português e ao nível do Exército.



Arquitetura Unificada de Comunicações para viaturas militares táticas

Tenente-Coronel Tm Paulo Margarido

Adjunto do Gabinete de Planeamento e Coordenação de Projetos da DCI

Com o propósito basilar de assegurar da entrega a mensagem ao destinatário, garantindo sempre uma execução em cumprimento da urgência necessária, tem sido um desafio crescente integrar a plenitude de sensores e as necessidades de informação dos principais utilizadores. Trata-se de um contínuo exercício indutivo, com vista a antever as necessidades fundamentais que se poderão apresentar, gradual e sucessivamente, acrescentando capacidades mediante os desenvolvimentos tecnológicos e maximizando o parco investimento disponível nas mais valias possíveis.

Num cenário de evolução rápida e exponencial, em que a celeridade do surgimento de novas tecnologias emergentes e transformativas suplanta a capacidade, dotação orçamental e rapidez na efetiva adoção das novas soluções, ainda que com o esforço contínuo de uma equipa que acompanha os vários desenvolvimentos da indústria, também com um número limitado de efetivos (como perpassa nos vários quadros do exército), verifica-se que o material recebido muitas vezes não representa já uma solução atualizada ou *state of the art*.

O projeto *Combat Net Radio* (CNR), em fase de desenvolvimento, é um exemplo concreto do referido, que conta com um rádio eleito (PRC-525 [1]) que disponibiliza comunicações seguras (SECOM-V), como principal meio de comunicação e que está ao serviço há tempo suficiente para ser sujeito a uma atualização de meio do tempo de vida. O referido rádio não permite a utilização da única forma de onda segura disponível nos rádios dos baixos escalões (RBE [2]) (onda TNW-50), tornando assim impossível a comunicação entre esse projeto e os baixos escalões.

Numa análise mais recente do projeto CNR, com vista à modernização e atualização do projeto, face ao contexto evolutivo acima descrito, foram, assim, encontradas algumas lacunas nos canais de comunicação utilizados (figura 1) entre as viaturas e os combatentes, bem como de acesso à estrutura central de comunicações, o SIC-T [3].

Desta forma surgiu a ideia de criação de uma arquitetura unificada de comunicações (figura 2) para viaturas militares táticas, em complemento ao projeto CNR, com vista a equipar as viaturas de combate do QOM [4] das unidades de manobra, desde o mais baixo escalão, para que possam utilizar as diferentes ferramentas de C2 [5] com o máximo proveito e flexibilidade para os combatentes.

Neste sentido, e com base nas opiniões dos operadores, face às limitações encontradas do uso da arquitetura do CNR em desenvolvimento, foi explorado o conceito da criação de uma arquitetura genérica, onde a estrutura de comunicações das viaturas de combate se possa basear independentemente da tipologia, permitindo uma mais ágil transformação entre tipologia e, bem assim, canais logísticos mais leves.



Figura 1 - Lacunas nos canais de comunicação utilizados

[1] - <https://www.eid.pt/what-we-do/land/prc-525-combat-net-radio/>

[2] - Radio de Baixo Escalão (R&S TR5000H)

[3] - Sistema de Informação e Comunicações – Tático (PDE 6.00)

[4] - Quadro Orgânico de Material

[5] - Comando e Controlo



O racional utilizado para esta nova arquitetura genérica foi o de utilizar os meios já disponíveis no Sistema de Combate do Soldado (SCS) e no SIC-T, tentando maximizar as larguras de banda disponíveis nos diferentes tipos de meios rádio, e o de ter por base a utilização dos meios do SCS durante toda a operação. A utilização dos meios SCS permite evitar a troca de meios de comunicação dentro e fora da viatura e integrar todos os meios com um equipamento já em uso (o ICC-401 [6]), permitindo assim a utilização de canais de voz entre todos os meios de comunicação rádio, com independência dos mecanismos concretamente utilizados (SECOM-V ou TNW-50) nas comunicações seguras.

Esta arquitetura única não está totalmente finalizada, encontrando-se em curso desenvolvimentos relevantes na atualização do rádio PPRC-525, que permitirá a inclusão da capacidade de implementação da forma de onda TNW-50, compatibilizando o PPRC-525 com o RBL [7] e o RBE [8], sem qualquer perda na sua função principal.

Outro dos projetos (figura 3) em maturação no âmbito da arquitetura única, mas cuja implementação se prevê como possível num prazo mais curto, é o de inclusão dos acessórios de passagem de voz, dados e energia dos rádios de combate para a viatura.

Efetivamente, o protótipo que permitirá essa inclusão encontra-se em fase final de desenvolvimento e permitirá aos militares, ao entrar na sua posição na viatura, usufruírem de uma comunicação filar para canais de voz entre a tripulação e o recarregamento de baterias dos equipamentos que estão a cargo do militar, mantendo, deste modo, as comunicações de voz e abrindo canais mais amplos para a transferência de dados.

Um dos principais fatores deste desenvolvimento, que está já em fase de validação, é o encaixe, que se pretende que assuma simplicidade (permitindo a sua operação com luvas), baixa complexidade (não requerendo a dispersão da atenção do militar para o operar), robustez (procurando assegurar o máximo de durabilidade possível nas circunstâncias mais extremas) e rápido desacoplamento (permitindo ao militar uma saída rápida e imediata para fora da viatura, sem precisar de qualquer procedimento moroso).

Ainda que com as limitações de efetivos e de investimento, espera-se que os projetos em curso, com assento numa arquitetura única, elevem as capacidades de comunicação nas viaturas militares e, com isso, possam ampliar a facilidade de comunicações entre os vários meios rádio existentes, criando soluções que melhoram a interação dos utilizadores com os equipamentos e diminuem os tempos de ação/reação, tendo em vista a crescente integração de meios no campo de batalha de suporte ao comando e controlo.

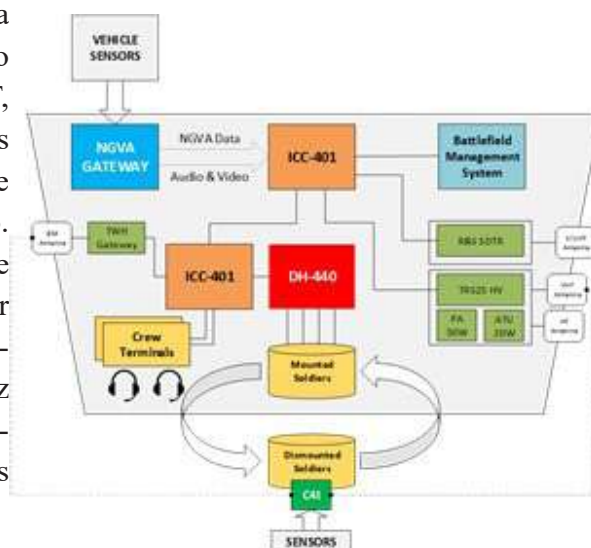


Figura 2 - Diagrama de blocos da arquitetura única



Figura 3 - Projeto Dismounted Soldier System - Veicular Integration

[6] -Sistema IP de intercomunicação

[7] -Radio de Baixo Escalão (R&S TR5000H)

[8] -Sistema de Informação e Comunicações – Tático (PDE 6.00)



Desenvolvimento Aplicacional: On-premises vs Cloud

Tenente RC Fábio Domingues

Desenvolvimento Aplicacional CDABI - DCI

Introdução:

O desenvolvimento aplicacional é uma parte essencial do ciclo de vida do *software*, e a escolha entre implementações on premises e na cloud desempenha um papel crucial nesse processo. Ambos os modelos apresentam características distintas que podem influenciar as decisões tomadas pelas organizações ao desenvolver *software*.

On Premises:

O desenvolvimento on premises refere-se à prática de alojar e operar *software* em servidores locais, geralmente dentro das instalações físicas de uma organização. Isso envolve investimentos em *hardware*, infraestrutura de rede e mão de obra especializada para gerenciar e manter os sistemas.

Vantagens:

1. Controle total: As organizações têm controle total sobre a infraestrutura, permitindo ajustes específicos de acordo com as necessidades;
2. Segurança percebida: Muitas vezes, é percebido como mais seguro devido à proximidade física e controle direto nos servidores.

Desvantagens:

1. Custos Iniciais Elevados: Requer investimentos substanciais em hardware e software desde o início;
2. Escalabilidade Limitada: A escalabilidade pode ser um desafio, pois a expansão exige mais investimentos em *hardware*.

Cloud:

O modelo de desenvolvimento na *cloud* envolve a utilização de recursos de computação remotos, geralmente fornecidos por provedores de serviços em nuvem, como *Amazon Web Services (AWS)*, *Azure da Microsoft* ou *Google Cloud*. As aplicações são implantadas e geridas em servidores remotos, acessíveis pela internet.

Vantagens:

1. Escalabilidade: Pode escalar facilmente para cima ou para baixo, com base nas demandas, sem a necessidade de investimentos significativos em infraestrutura;
2. Custos Operacionais: Reduz custos operacionais, pois a organização paga apenas pelos recursos que consomem.

Desvantagens:

1. Dependência da conectividade: A disponibilidade da aplicação depende da conectividade com a internet;
2. Segurança percebida: Algumas organizações ainda têm preocupações sobre a segurança dos dados na cloud.



Comparação:

O desenvolvimento on premises refere-se à prática de alojar e operar software em servidores locais, geralmente dentro das instalações físicas de uma organização. Isso envolve investimentos em hardware, infraestrutura de rede e mão de obra especializada para gerenciar e manter os sistemas.

1. Custos:

- a. *On Premises*: Altos custos iniciais, mas despesas operacionais relativamente estáveis;
- b. *Cloud*: Custos operacionais mais baixos, pagos conforme o uso, mas potencialmente maiores ao longo do tempo.

2. Escalabilidade:

- a. *On Premises*: A escalabilidade pode ser cara e demorada;
- b. *Cloud*: Escalabilidade rápida e eficiente.

3. Controle e Segurança:

- a. *On Premises*: Controle total, percepção de maior segurança;
- b. *Cloud*: Menos controle direto, mas os provedores de cloud investem fortemente em segurança.

4. Implementação e Manutenção:

- a. *On Premises*: Requer gestão dedicada e atualizações frequentes;
- b. *Cloud*: Atualizações automáticas e manutenção é gerido pelo provedor.

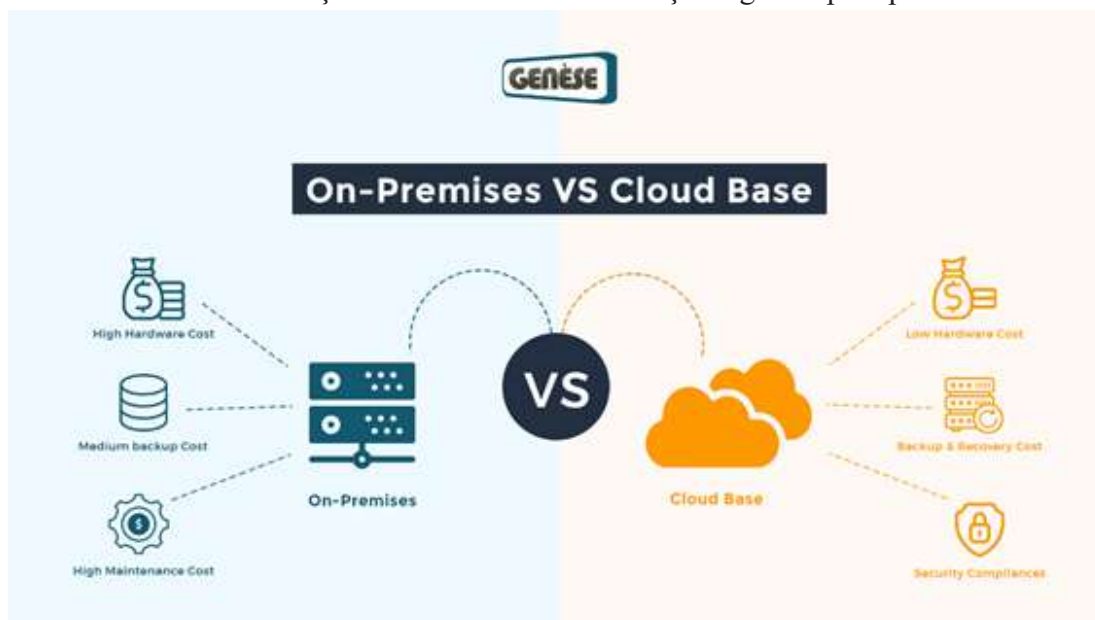


Figura 1 - On-premises VS Cloud Base

Conclusão:

A escolha entre desenvolvimento on premises e cloud depende das necessidades específicas de cada organização. Enquanto o on premises oferece controle total, a *cloud* proporciona flexibilidade e eficiência de custos. A decisão final deve levar em consideração fatores como orçamento, escala, requisitos de segurança e preferências organizacionais. Em muitos casos, uma abordagem híbrida pode ser a solução ideal, combinando o melhor dos dois mundos para otimizar o desenvolvimento aplicativo.



A Guerra de Informação porque é hoje mais importante que nunca?

Tenente-Coronel Tm Monteiro Fernandes

Chefe da Repartição de Guerra de Informação da DCI

Podemos dizer que a Guerra de Informação (GI) é já um conceito antigo, mas simultaneamente é também um conceito novo. Neste artigo, faz-se uma breve reflexão sobre este conceito, tentando clarificar a sua importância nos dias de hoje e as implicações que pode trazer para o Exército.

Começamos inicialmente pelas definições. Recorrendo à incontornável doutrina Americana, foi no final do século passado que começou a ser desenvolvida uma base doutrinária específica para a GI, vocacionada para sistematizar a utilização da informação no futuro campo de batalha. Concretamente, o Manual de Campanha FM 100-6 (*Information Operations*), publicado em 1996 pelo Exército dos EUA, aborda as alterações geoestratégicas e tecnológicas que a emergência da GI coloca ao ambiente operacional, definindo a GI como “conjunto de ações desenvolvidas para obter a superioridade de informação, afetando a informação, processos baseados em informação, sistemas de informação e redes baseadas em computadores de um adversário, enquanto se defende a nossa informação, processos baseados em informação, sistemas de informação e redes baseadas em computadores” [1]. Contudo, nesse mesmo manual, o Exército Americano, reconhecendo que a GI assim definida pelo Departamento de Defesa, se centra de forma mais restrita no impacto da informação durante um conflito real, optou por adotar uma abordagem um pouco mais ampla do impacto da informação nas operações terrestres, utilizando antes o termo Operações de Informação. Ao longo dos anos seguintes, a expressão GI foi sendo utilizada em alguns contextos com maior ou menor relevo. Se olharmos ao FM 3-0 (*Operations*), a expressão GI não aparece nas versões de 2001 nem na de 2008, mas aparece por quatorze vezes na edição de 2017 e por quarenta vezes na versão atual do manual publicado em 2022, o que reflete um ganhar de importância deste conceito para o Exército Americano. Isto acontece no contexto da mudança da doutrina no sentido de operações multi-domínio, o que aumentará o papel da informação no combate.

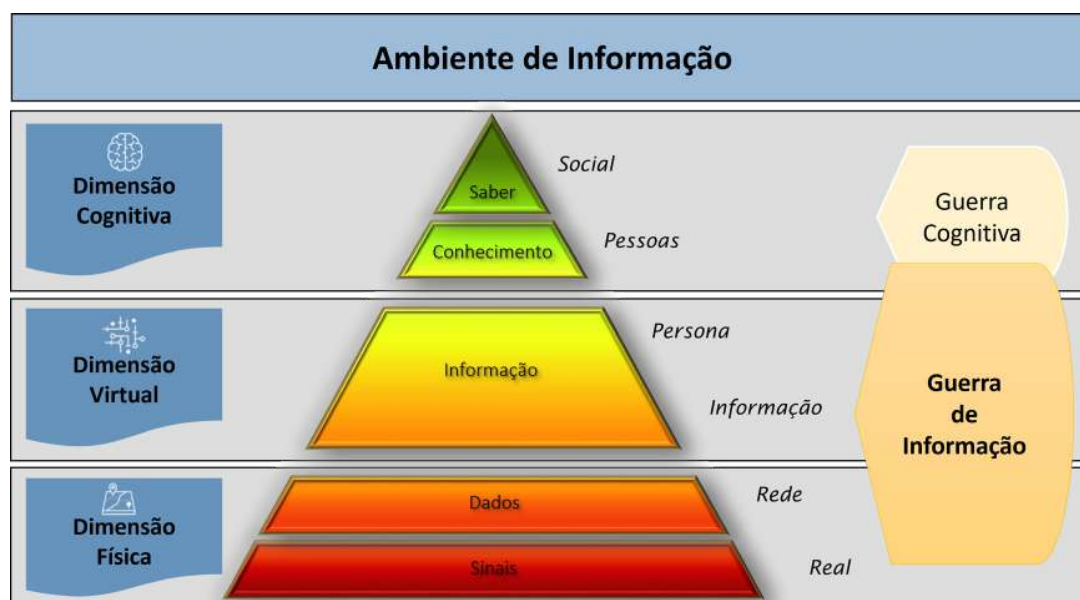


Figura 1 – Ambiente de informação

[1] - Tradução constante dum Estudo de 2011 do EME intitulado “Superioridade de Informação: um objetivo estratégico para o Exército”



Assim, importa compreender melhor o ambiente de informação, conforme preceituado na doutrina [2], observando a Figura 1, onde é possível notar as três diferentes dimensões desse ambiente, alinhadas com a designada “pirâmide cognitiva”, construída a partir dos seus níveis de abstração (sinais, dados, informação, conhecimento e sabedoria).

É, pois, a capacidade de atingir e manter a superioridade de informação que permite moldar o ambiente de informação, potenciando a realização de outras ações com vista a alcançar os efeitos pretendidos sobre um determinado adversário e em última análise conduzir à superioridade da decisão. De notar também que a GI está hoje muito associada à utilização do ciberespaço, pelo relevo que este ocupa no ambiente de informação. Sublinhar ainda que, no âmbito da GI podem decorrer operações de ataque e defesa, destinadas a afetar os sistemas dos potenciais adversários e a proteger os nossos sistemas, principalmente os de comando e controlo.

Quando pensamos em estratégia, pensamos nos fins, nas formas/métodos e nos meios. Nesse sentido podemos dizer que o conceito de GI é uma forma de efetivar e executar a estratégia. Para tentar sintetizar o conceito de GI, referir que este expressa, acima de tudo, a ideia de conflito e a posição que a informação ocupa neste contexto. Logo, poderá até dizer-se que é um conceito tão antigo como a guerra, mas que acontece de uma forma muito mais visível e numa escala muito mais ampla nesta nova era da informação, que proporciona um ambiente de informação que é globalmente acessível e através do qual as mensagens são facilmente difundidas. Portanto, é também um conceito muito atual.

Mensagens como *Make Rome Great Again* podem-nos soar familiares nos tempos modernos [3]. Contudo, já líderes e imperadores romanos ambiciosos usaram a narrativa, temas e mensagens-chave para ganhar poder, quando o declínio era criticado, a mensagem passava a ser: oferecer uma renovação do império. Marco Aurélio, por exemplo, utilizou este facto de forma positiva: falou do declínio e da crise para reforçar os laços que mantinham unidos os seus súbditos. Nos tempos mais recentes temos a narrativa ocidental da guerra global ao terrorismo, em que se oferece um futuro de democracia, esperança, liberdade de expressão, etc., sendo que, em oposição, os terroristas oferecem um futuro de repressão, medo e pobreza.

A comunicação estratégica e a GI tratam de moldar e mudar o comportamento, usando linguagem, ação, imagens ou símbolos para alcançar um efeito ou um estado final desejado. Porém, não nos devemos amarrar às definições de GI, a tecnologia mudou as formas e os meios utilizados na guerra, mas não mudou a natureza da guerra! A trindade de *Clausewitz* – violência irracional / ódio, acaso / oportunidade e a razão [4] permanecem. E podemos observar fatores de GI em todas estas três características: sobre a vontade de lutar, sobre acontecimentos do acaso e imprevisíveis e no propósito político.

A informação sempre foi uma característica da guerra e das operações, apresentando hoje, uma relevância sem precedentes nos conflitos armados. Em alguns casos, as operações cinéticas requerem prioridade. Em outros, será a informação a ter essa prioridade. Antigamente os militares usavam a informação para justificar a ação cinética, mas, hoje em dia, a necessidade estratégica pode reverter isso, ou seja, a ação cinética pode servir de suporte da narrativa.

[2] - Publicação Doutrinária do Exército, PDE 6-0 Comunicações e Informação, de agosto de 2023

[3] - Parte deste artigo foi baseado nas notas de uma comunicação feita por James Farwell (2021) no comando ACT da NATO

[4] - Em inglês: Will, Change (uncertainty/friction) e Reason



Mas o que é diferente agora? Ora, num mundo globalmente ligado e em rede, onde cada sala de estar pode ser um espaço de batalha, a informação pode desempenhar um papel igual ou superior à ação cinética. Poderemos ser levados a pensar que as redes sociais são uma novidade. Contudo, elas não são novas! Martinho Lutero, por exemplo, aproveitou-as para dar início à sua reforma. Napoleão capitalizou-as no século XVIII para ganhar poder. Ou seja, as redes e a conectividade definem a natureza da era atual, as ligações aumentam a nossa capacidade de comunicar e de criar novas ligações. Por isso, essa conectividade permite que pequenas peças se combinem e se transformem em coisa mais poderosas. Assim, ao se alcançar o domínio da informação, torna-se possível conduzir a mensagem que mais nos convém.



44.  memSagem

SIGNAL INTELLIGENCE – RELIABLY IDENTIFY THE RIGHT TRACK IN THE SPECTRUM.

Intercepting signals is less relevant today than selecting the right "grain" among the huge flow of incoming data. Rohde & Schwarz supports various missions by providing all-in-one signal intelligence solutions – from sensor technology to signal processing and signal analysis tools – that provide a solid basis for political and military decisions. For decades, decision makers in command have been relying on the results of analysis solutions from Rohde & Schwarz.

www.rohde-schwarz.com/sigint



ROHDE & SCHWARZ

Make ideas real





A relevância do CSO alternativo na resiliência dos SIC [1] do Exército e das Forças Armadas em geral

Major Tm José Paiva

2º Cmdt do Grupo de Controlo e Gestão de Sistemas do Centro de Transmissões do Exército (CTE)

Enquadramento

A designação Centro de Sistemas Operacionais (CSO) foi utilizada em 17set12 quando se inaugurou o Centro de Dados (*Data Center*) principal do Exército no PM 042 – Quartel de Sapadores em Lisboa, nas atuais instalações do Centro de Transmissões do Exército (CTE), com o objetivo de dotar o Exército de uma capacidade centralizada de processamento e armazenamento de informação necessária ao seu Comando e Controlo (C2).

Os *Data Centers* são instalações físicas centralizadas constituídos por sistemas de computadores, sistemas de armazenamento, comunicações (entre outros) utilizados para processar, armazenar e gerir grandes quantidades de dados, bem como para fornecer serviços de uma forma contínua num ambiente seguro e controlado.

Uma das classificações frequentemente utilizada é de acordo com a disponibilidade e confiabilidade de um *Data Center*, com base no sistema de tiers [2], desenvolvido há mais de 25 anos pelo *Uptime Institute*. Avalia, essencialmente, aspetos relacionados com comunicações, ações de manutenção e sistemas de apoio (energia e climatização), podendo dizer-se que é uma medida de “quão à prova de falhas” um *Data Center* é. Segue o resumo dos 4 níveis:

- *Tier I*: Básico - com proteção contra falhas humanas, mas não contra falhas inesperadas;
- *Tier II*: Redundância simples – oferece redundância para melhor manutenção e segurança contra interrupções;
- *Tier III*: Manutenção concorrente – mantém a disponibilidade mesmo durante uma manutenção;
- *Tier IV*: Tolerante a falhas - sistemas independentes e fisicamente isolados com tolerância a falhas.

Um *Data Center* alternativo é uma instalação secundária que é utilizada normalmente para recuperação de desastres [3] (DR) em caso de falha do *Data Center* principal.

Seguem alguns aspetos importantes a reter para a implementação de um *Data Center* alternativo:

a. Localização geográfica

O *Data Center* alternativo deverá estar, de preferência, localizado a uma distância segura do *Data Center* principal para evitar que os mesmos eventos (por exemplo uma catástrofe natural) tenham impacto em ambos os locais.

b. Replicação de Dados

Deverá haver uma replicação contínua e eficiente dos dados entre o *Data Center* principal e o secundário, de forma a estarem atualizadas e prontas a utilizar em caso de falha.

c. Capacidade de Recuperação Rápida

O *Data Center* secundário é fundamental num plano de DR, permitindo a recuperação rápida dos serviços em caso de eventos catastróficos, como incêndios, terremotos, inundações, etc.

[1] - Sistemas de Informação e Comunicações

[2] - Tiers em *Data Centers* referem-se a um padrão de classificação desenvolvido pelo *Uptime Institute* para descrever a confiabilidade e disponibilidade de um *Data Center*.

[3] - Utilizado geralmente o termo em inglês *Disaster Recovery*.



d. Testes regulares

Periodicamente, devem ser realizados testes (simulacros) de falha do *Data Center* principal para verificar se os procedimentos de recuperação estão bem documentados e a funcionar como esperado.

e. Balanceamento de carga

Em algumas situações, o *Data Center* secundário pode ser utilizado para distribuir carga, proporcionando melhor desempenho e escalabilidade.

f. Segurança

A segurança é um aspeto fundamental, de modo a garantir a integridade, confidencialidade e disponibilidade dos dados. Para garantir a capacidade de DR e continuidade de negócio no C2 do Exército foi edificado o Centro de Sistemas Operacionais alternativo (CSOa) no Campo Militar de Santa Margarida (CMSM), nas instalações do antigo Destacamento de Comunicações e Sistemas de Informação (CSI) Centro (Ed nº 70 do CMSM). A escolha desta localização para o CSOa deveu-se sobretudo aos seguintes fatores:

- Redundância de ligações e de equipamentos, garantindo a sobrevivência do sistema: o CMSM, para além das ligações através de fibra ótica, estabelece ligações redundantes por Feixes Hertzianos, por caminhos alternativos, para Norte, Sul e Lisboa;
- Alta disponibilidade de largura de banda (LB): o CMSM é a infraestrutura militar com maior capacidade de estabelecer comunicações de alto débito através de caminhos alternativos fora da região de Lisboa;
- Segurança física: localizado dentro de uma Unidade Militar;
- O CMSM situa-se numa região com baixo índice de risco a catástrofes naturais;
- Interligação com antena para ancoragem de comunicações satélite de alto desempenho (edificação da capacidade MILSATCOM pelo Estado-Maior General das Forças Armadas [EMGFA]).

Estado atual

As obras para a edificação do CSOa foram concluídas em junho de 2023, projeto conduzido pela DCI, com apoio da DIE, utilizando verbas da LPM do projeto “EXE-02 – Sistemas de Informação e Comunicações Operacional (SIC-Op)”, no âmbito da capacidade de C2 Terrestre. A DIE ficou com a responsabilidade da infraestrutura física, climatização, deteção e extinção de incêndios e a DCI com a infraestrutura de comunicações, tecnologias de informação, videovigilância e controlo de acessos eletrónico e energia.

O estado atual do CSOa é o seguinte:

- Infraestrutura física

- o Edifício da Torre de Comunicações (EdTC) para a componente de energia (gerador e UPS) e equipamentos ativos para o *Core* da Rede de Dados do Exército (RDE);

- o Parte do Ed70 do CMSM, constituída por 2 salas para o Domínio Não Classificado (DNClas) e Domínio Classificado (DClas) da RDE. A sala do DNClas tem uma área de 6,850x4,050m e do DClas 3,300x4,030m.

- Energia

- o Todos os bastidores do CSOa são alimentados por dois circuitos de energia suportados em duas UPS independentes;

- o O edifício da Torre de Comunicações é alimentado apenas por uma linha de baixa tensão;

- o Gerador (com potência de 125 KVA e depósito com capacidade para 500 Litros) para garantir energia suportada às duas UPS.



- Aquecimento, Ventilação e Ar Condicionado (AVAC)
 - o O sistema de controlo de temperatura/humidade é constituído por 4 máquinas de ar condicionado;
 - o Existe um processo aquisitivo para um novo sistema constituído por 2 máquinas.
- Sistema de deteção e extinção de incêndio
 - Implementado sistema de deteção e extinção de incêndio através de agentes gasosos.
- Videovigilância e controlo de acessos
 - Implementado sistema de videovigilância e controlo de acessos e integrado no Sistema Integrado de Controlo de Acessos e Videovigilância do Exército (SICAVE).
- Comunicações
 - o Fibras óticas redundantes e por caminhos distintos entre o EdTC e os dois bastidores principais, estes também redundantes;
 - o Nas Salas do DNClas e DClas, todos os bastidores estão ligados por fibras óticas redundantes;
 - o No EdTC existem 2 equipamentos de rede L3 de Core de Santa Margarida. Estes estão ligados, em redundância, a dois equipamentos de rede que são responsáveis por todas as comunicações de entrada e saída do CSOa.
- Sistemas de Informação
 - o No DNClas já existe um novo sistema de hiperconvergência com capacidade idêntica ao do Centro de Sistemas Operacionais principal (CSOp). Contudo, ainda é necessário algum investimento na solução de virtualização para poder efetuar a replicação dos servidores entre o CSOp e CSOa;
 - o No DClas está a ser implementado o sistema de hiperconvergência que estava anteriormente no DNClas.

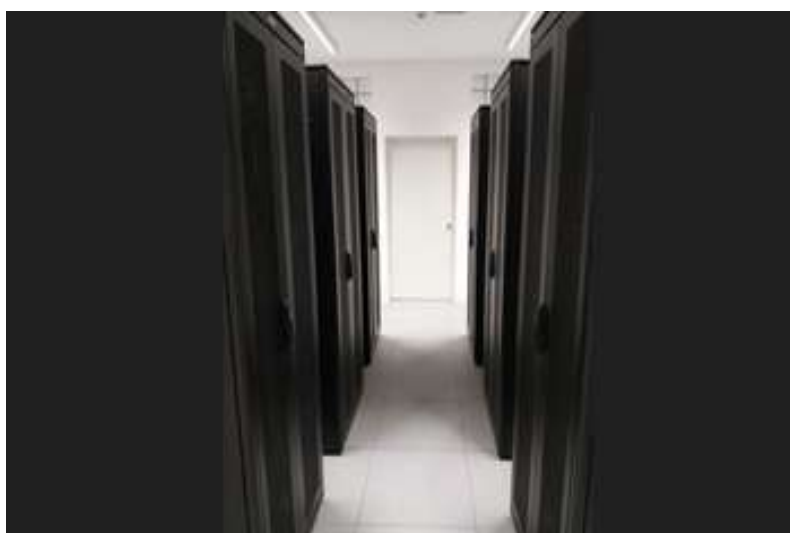


Figura 1 – Sala do DNClas do CSO



Estado final desejado

O objetivo principal após a edificação do CSOa é torná-lo mais robusto, e implementar uma arquitetura física e lógica que permita alcançar um *Recovery Point Objective* (RPO) [4] e um *Recovery Time Objective* (RTO) [5] o mais baixo possível. Como valores de referência, pretende-se um RPO de 5 minutos e um RTO de 15 minutos (estes valores poderão baixar para menos de 1 minuto nos serviços considerados críticos, como o correio eletrónico e Bases de Dados).

Para que isso seja possível é necessário o seguinte investimento:

- Sistemas de apoio

A nível de energia é necessário a instalação de um novo ramal de energia suportada em gerador e deslocalizar uma das UPS para outro local físico. Ao nível dos AVAC é recomendado adquirir mais uma Unidade.

CSOa		
	Atual	Desejado
Comunicações	TIER IV	TIER IV
Sistemas de apoio		
• energia	TIER II	TIER IV
• AVAC	TIER II	TIER IV

Tabela 1 – Classificação do CSOa com base nos tiers

- Comunicações

Importante existir ligação de fibra ótica alternativa entre o CSOp e CSOa por caminho distinto.

- Sistemas de Informação

o Aquisição de balanceadores de carga e upgrade da licença da plataforma de virtualização, para permitir a replicação das máquinas entre o CSOp e o CSOa;

o Robustecer a solução de *backups*, de forma a ter capacidade de efetuar cópias de segurança para disco e tape em ambos os CSO;

o Servidores para replicar as máquinas de/para acesso ao exterior (envio e receção de emails do exterior, site do Exército na internet, etc);

- Segurança e proteção de perímetro

o Equipamentos de proteção de perímetro (acesso através de VPN)

o Equipamentos cripto (para o DCIas)

Para além do investimento do Exército, o EMGFA tem de estender a interligação dos Ramos bem como a ligação à rede segura nacional (POP EMGFA) em Santa Margarida, de modo a assegurar o DR de serviços como o *Military Message Handling System* (MMHS), Sistema Integrado de Gestão da Defesa Nacional (SIG-DN), Processo Clínico Único (PCU), entre outros.

A solução escolhida para operacionalizar um DR é o *VMWare Site Recovery Manager* (SRM) [6]. O SRM é um orquestrador desenhado para DR que trabalha com a infraestrutura de virtualização da *VMWare* (que já existe). Esta solução automatiza todo o processo de DR em ambientes virtualizados de forma a garantir a continuidade de negócios das organizações.

[4] - RPO é o intervalo de tempo que uma organização está disposta a perder dados em caso de desastre.

[5] - RTO é o tempo máximo que uma organização está disposta a tolerar para recuperar os serviços após uma interrupção.

[6] - Esta foi a solução escolhida pelo facto de toda a infraestrutura de virtualização do Exército ser VMWare.



Em caso de falha do CSOp, executa-se um procedimento manual simples (carregar num botão de pânico) no CSOa para iniciar o processo de *failover* [7] e iniciar todo o processo de automação definido no SRM, de forma a restabelecer todos os serviços com um RTO de, no máximo, 15 minutos.

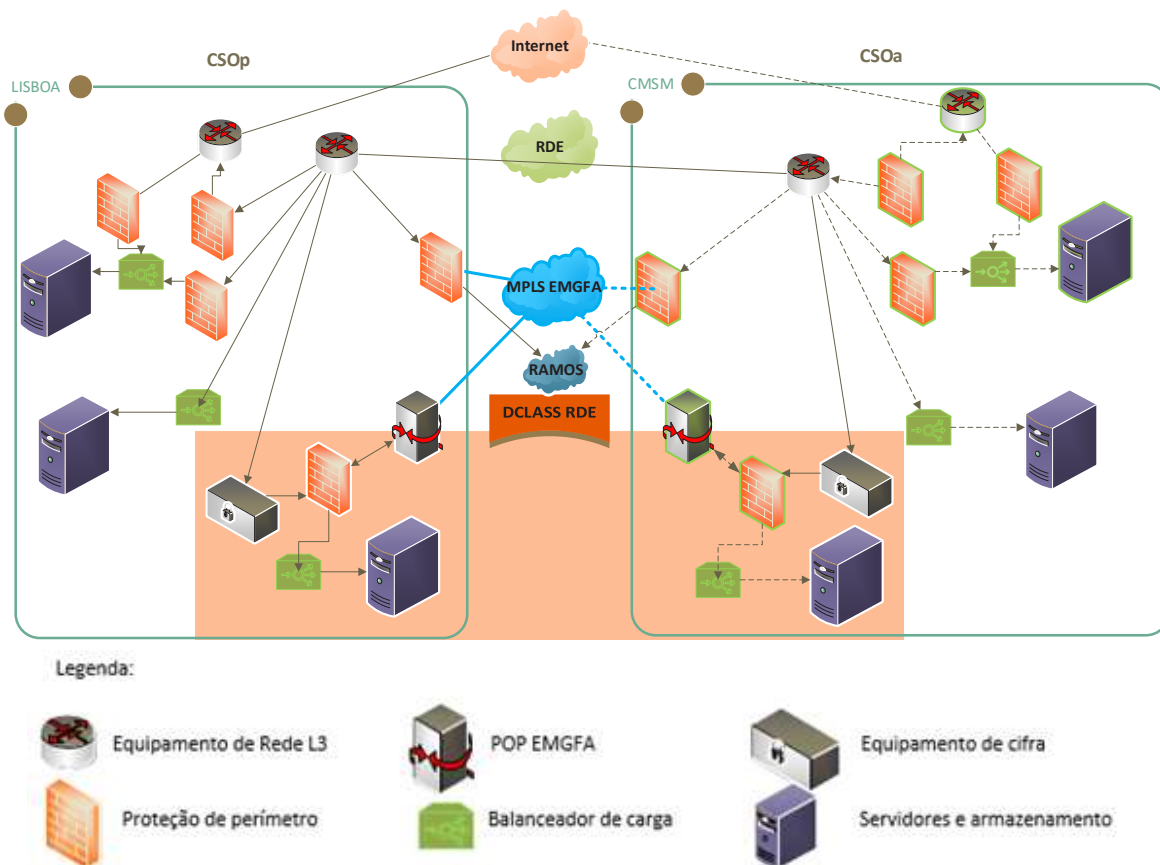


Figura 2 – Diagrama lógico do estado final desejado

Conclusões

Para a edificação do CSOa no CMSM, de acordo com o estado final desejado, ainda será necessário um investimento substancial, nomeadamente ao nível dos Sistemas de Informação e equipamentos de proteção de perímetro. Contudo, o mais difícil já foi feito, que foram as obras no Ed. nº 70, permitindo ter uma área controlada e com os requisitos técnicos necessários para implementar um Data Center secundário.

O objetivo futuro é tornar o CSOa mais robusto, procurando um RPO e RTO mais baixos. Para isso, são necessários investimentos, de forma a poder adquirir toda a componente de sistemas de informação, proteção de perímetro e sistemas de apoio para implementar a solução final, de acordo com o diagrama apresentado na Figura 2.

A solução escolhida para operacionalizar o DR é o *VMWare SRM*, que automatiza o processo de recuperação em ambientes virtualizados.

A implementação efetiva do CSOa é vital para a resiliência dos SIC do Exército, assegurando a continuidade das operações em situações de falha do CSOp. Pelo facto de existir ligações de fibra ótica no CMSM aos equipamentos do EMGFA e da edificação da capacidade MILSATCOM, este CSOa poderá servir para garantir, também, uma resiliência ao nível das Forças Armadas.

[7] - Termo utilizado para a transição automática de uma operação ou serviço de um componente primário para um secundário.



Comunicar com Fiabilidade, Segurança e Resiliência

A rede SIRESP é a rede de comunicações exclusiva do Estado Português para o comando, controlo e coordenação de comunicações em todas as situações de emergência e segurança, que responde às necessidades dos mais de 40.000 utilizadores e suporta anualmente um número superior a 224 milhões de chamadas o que permite incrementar os níveis de confiança, segurança e de bem-estar das populações.



Projetos SIRESP



Lab

Estimular a Inovação
e a ligação à Indústria



Desafio Inovação

Promover ligação
ao meio académico



Bootcamp

Geração e Validação
de Competências



Tech Days

Fórum aberto de discussão
de ideias e soluções



Academia

Capacitação
da comunidade

Saiba mais sobre a SIRESP, S.A. em

www.siresp.pt



Participação do Exército nas edições do SIRESP Bootcamp

Tenente Tm Carlos Gomes
Membro da EqpProj SIC-T/DCI

Introdução

O Sistema Integrado de Redes de Emergência e Segurança de Portugal (SIRESP) é a rede de comunicações para o comando, controlo e coordenação de comunicações em todas as situações de emergência e segurança, do Estado Português. Atualmente o SIRESP é utilizado por diversas organizações como a Polícia de Segurança Pública (PSP), a Guarda Nacional Republicana (GNR), Corpos de Bombeiros, Instituto Nacional de Emergência Médica (INEM), entre outros.



Figura 1 – Exemplos de entidades utilizadoras de equipamentos SIRESP

Dada a grande abrangência e importância do sistema, a entidade responsável por planear, gerir, manter e modernizar a rede (SIRESP, S.A), desenvolveu três edições do SIRESP *Bootcamp*, nas quais o Exército tem vindo a participar, nomeadamente, através da DCI:

1ª Edição: Açores - 17 a 21 de outubro 2022

2ª Edição: Madeira - 27 a 31 de março 2023

3ª Edição: Algarve - 20 a 24 de novembro de 2023

Estes *Bootcamps* têm como finalidade primária o desenvolvimento de competências, a discussão de conceitos e temas de interesse para a Comunidade SIRESP, tendo em vista quer a sua demonstração e aplicação prática como a sua validação operacional, bem como a aquisição, geração e validação de competências, inovação, capacitação e reforço da disponibilidade, resiliência e segurança da rede SIRESP.

Demonstração de Capacidades – *Bootcamp* Portimão

Na 3ª Edição do *Bootcamp* foi utilizado o diagrama de rede visível na Figura 2, constituído por 2 locais, Portimão e Lisboa. Em Lisboa, foi montado um Posto de Comando Tático, no Comando das Forças Terrestres (CFT), equipado com o sistema de Comando e Controlo (C2) *Battlefield Management System* (BMS), interligado à equipa em Portimão através da Rede de Dados do Exército. Por sua vez, a equipa de Portimão é conectada à RDE através de *Virtual Private Network* (VPN) fornecido pela *firewall Checkpoint*. Através de intercomunicadores ICC-401 da EID, foi possível integrar várias redes e equipamentos que não são diretamente interoperáveis, isto é, foi possível comunicar entre diferentes redes, cujos equipamentos não são capazes de comunicar entre si.



Esta capacidade pode ser particularmente interessante em situações de catástrofe, em que há necessidade de articular esforços entre diferentes entidades, cada uma com as suas redes e os seus equipamentos, como é o exemplo das redes militares (ramos das Forças Armadas) e redes civis. Foi possível interligar telemóveis a comunicar em rede 5G, com uma viatura URO VAMTAC do Regimento de Comandos (equipada com o rádio tático PRC-525), com equipamentos SIRESP, de tecnologia *Terrestrial Trunked Radio* (TETRA), com os novos rádios de baixo escalão (RBE).

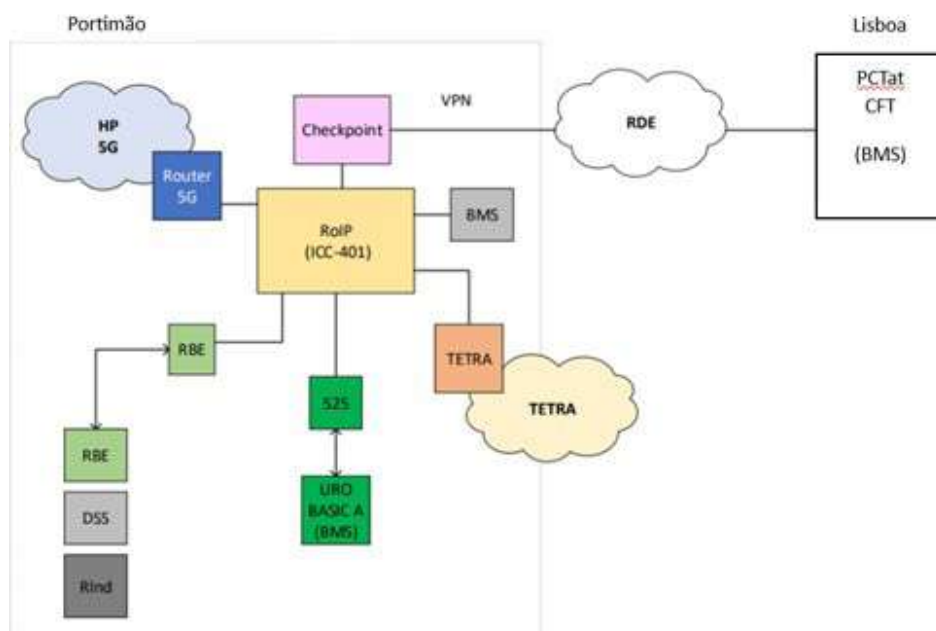


Figura 2 – Diagrama do sistema

Foram demonstradas capacidades de *Friendly Force Tracking* através dos novos rádios do sistema de Comando, Controlo, Comunicações, Computadores e Informações (C4I), o HR5000 da *Rohde & Schwarz*, com a função de rádio de baixos escalões (RBE) e o TWH-104R da EID, com a função de rádio individual (RInd). Ambos os rádios possuem antenas com capacidade de posicionamento (GPS), demonstrando as posições dos militares e viaturas através dos sistemas de Comando e Controlo (C2) *Battlefield Management System* (BMS) e *Dismounted Soldier System* (DSS).

Conclusão

Estes exercícios de interoperabilidade são eventos de grande importância para o Exército, onde é possível desenvolver conhecimento e demonstrar a capacidade de interligação de redes e equipamentos do Exército com redes e equipamentos de outras entidades, permitindo a que todos os combatentes apeados, viaturas ou postos de comando, comuniquem com os restantes meios externos à instituição.



Figura 3 – Fotografias dos 3 eventos Bootcamp SIRESP



As comunicações no apoio de uma *Quick Reaction Force* no Teatro de Operações da República Centro Africana

Capitão Tm Aires Ceita
Chefe do Módulo CSI da 13ª FND RCA

Num Teatro de Operações (TO) tão exigente como a República Centro Africana (RCA), onde a infraestrutura de comunicações e o acesso à internet no país é ainda muito limitado, o módulo de comunicações tem um papel determinante para garantir o exercício do Comando e Controlo (C2) ao Comandante da Força e a toda a sua estrutura hierárquica na Missão Multidimensional Integrada das Nações Unidas (QRF/MINUSCA).

Inicialmente composto por oito militares, um oficial, três sargentos e quatro praças, para fazer face ao cumprimento de todas as tarefas, principalmente quando a força é projetada e tem objetivos a cumprir tanto na *Main Operation Base* (MOB) como na *Temporary Operation Base* (TOB), o módulo foi incrementado com mais um Sargento de Comunicações. Nesta tipologia de missão, recorrentemente com condições adversas e sem possibilidade de apoio externo, é fundamental 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 TO e o Território Nacional é essencial. Na MOB, essa valência é assegurada desde a primeira FND por uma ligação satélite, do tipo *Very Small Aperture Satellite Link* (VSAT), baseado numa antena GIGASAT e com uma largura de banda flexível consoante a disponibilidade da banda X atribuída à QRF por parte da DIRCSI/EMGFA. Quando em projeção, juntamente com a viatura de comunicações – Centro de Comunicações de Companhia (CCC) - a antena GIGASAT era também utilizada para a comunicação com o TN e para a MOB, sendo posteriormente substituída pela antena satélite *DataPath CCT 200*, também com capacidade para fornecer os serviços da RDE em projeção.



Figura 1 - Antena satélite DataPath CCT 200



O acesso à internet na MOB, quer para a rede de trabalho como para a rede de moral e bem-estar (*Welfare*) foi desde o início suportado pelo terminal satélite *AirBus* (antena GDSATCOM 1244) na banda C. Com uma largura de banda inicial de apenas 10MB/s, era possível, com alguma limitação, ter acesso à internet nos locais de trabalho e alojamentos. Através de um novo contrato com a *AirBus*, conseguiu-se aumentar a largura de banda para 20 MB/s. Sendo a RCA um país com uma deficiente infraestrutura de comunicações, fornecer internet de qualidade à QRF/MINUSCA continua a ser um dos grandes desafios para o Módulo CSI, tanto na MOB como na projeção. Recentemente umas das melhorias implementadas foi a aquisição do terminal satélite *Starlink* da *SpaceX*, que disponibiliza uma largura de banda muito superior à anterior e permite separar a rede de trabalho da rede *welfare*, o que não acontecia antes, por apenas existir um terminal satélite para o serviço de internet.

As comunicações internas da QRF/MINUSCA na RCA são baseadas em meios rádios, PRC-525, PRR H4855, ICOM, TETRA, telefones satélite IRIDIUM, THURAYA e rede GSM local. Os telefones satélite para além de comunicações internas permitem também estabelecer comunicações satélite de emergência para qualquer ponto do mundo. Todos os meios rádios em operação são essenciais para o C2 da Força, sendo o Rádio Tático 525 (PRC-525), instalado em todas as viaturas táticas e no Centro de Operações Tático (COT), o principal meio rádio de comunicação entre as viaturas, bem como entre estas e o COT. De forma a incrementar o C2 da Força em operação, no início do ano de 2021, o sistema BMS (*Battlefield Management System*) foi implementado nas viaturas táticas e no COT, tendo sido uma mais valia para o planeamento das operações e ainda para o comando e controlo de todos os movimentos. O BMS, num teatro de operações como o da RCA, representa uma ferramenta de C2 que fornece, a todos os elementos envolvidos nas operações, uma panorâmica completa do que está a acontecer, sem que estes sejam sobrecarregados com informação desnecessária, permitindo um desempenho eficiente.



Figura 2 - Comunicações internas numa viatura Tática Ligeira Blindada

A evolução da tecnologia e dos meios de comunicações são constantes e para garantir o apoio necessário a FND no cumprimento da sua missão no TO da RCA, é fundamental que os meios CSI, que auxiliam no exercício do C2 em operação, consigam acompanhar essa evolução.



O Módulo CSI da 3ªFND CAAtMec/ROU

Tenente Tm Pedro Costa

Comandante do Módulo CSI da 3ªFND CAAtMec/ROU

Fruto do presente conflito no leste da Europa entre a Rússia e a Ucrânia, Portugal, em 25 de maio de 2023, projetou mais uma Força Nacional Destacada (FND) para a Roménia, a 3ªFND Companhia de Atiradores Mecanizada, com o intuito de manter o compromisso com a *North Atlantic Treaty Organization* (NATO) e reforçar o flanco leste da Aliança Atlântica, no âmbito da *Enhanced Vigilance Activity* (EVA). A força encontra-se aquartelada no sul da Roménia, em Caracal, nas instalações do 1º Batalhão de Formação. Esta FND foi constituída por duzentos militares distribuídos pelas seguintes subunidades: Comando da Força, Companhia de Atiradores Mecanizada, Destacamento de Apoio, Módulo de Defesa Antiaérea, Módulo GeoMeteo e Módulo Conjunto de Informações. Organicamente esta FND integrou a Brigada Multinacional SE. Ao longo da missão, a Força participou em diversos exercícios conjuntos e combinados e atividades em vários locais e cidades romenas.



Figura 1 - ModCSI /3FND CAAtMec/ROU

O Módulo de Comunicações e Sistemas de Informação (ModCSI) da 3ª FND foi constituído por sete militares: um oficial, três sargentos e três praças. Destes elementos, seis são oriundos do Regimento de Transmissões e uma praça da Companhia de Transmissões da Brigada Mecanizada. Entre as várias funções do Módulo, destacam-se as seguintes: gere e opera o Centro de Comunicações da Força, garantindo o acesso à rede de dados do Exército e às redes classificadas (SECNET e NSWAN) via satélite ou Internet, contribuindo para o Comando e Controlo da força através da implementação do Sistema *Battlefield Management System* (BMS), o qual permitiu a interligação das Viaturas Blindadas de Rodas (17 viaturas da tipologia PANDUR e 5 viaturas da tipologia VAMTAC) e o Posto de Comando da Força assente em redes de comunicações rádio robustas, flexíveis e adequadas a cada operação com a capacidade de envio de voz e dados. O Módulo garantiu ainda o acesso dos militares à rede de *Wellfare* da Força, fazendo a alocação de largura de banda da mesma consoante o horário e a necessidade.



O Módulo dispôs de um Centro de Comunicações de Companhia (CCC), com meios de comunicações que permitiram dotar o Posto de Comando da Força com comunicações rádio e acesso à rede de dados do Exército através da antena satélite *Datapath CCT 200* ou de uma *checkpoint* com acesso à internet.

Durante a Missão, o Módulo participou em vários exercícios dos quais se realço o SCORPIONS LEGACY 23, maior exercício com forças da NATO na Roménia, no qual os militares de transmissões tiveram a oportunidade de testar a interoperabilidade dos meios de comunicações com outras forças, demonstrar capacidades e contactar com meios de comunicações das Forças aliadas, e contribuir muito significativamente para o desempenho positivo e visibilidade da 3ªFND. Realço ainda a realização do *Signals Exercise* (SIGEX) com o objetivo de dar formação de Transmissões aos militares da Força (Procedimentos de Cibersegurança na utilização de computadores na RDE, utilização do telefone *Iridium Extreme* PTT, operação do BMS, métodos de cifras de mensagens e operação do rádio P/PRC-525), treinar o envio de relatórios quer à voz via rádio, quer no BMS e por fim, testar comunicações HF com o Território Nacional (TN).



Figura 2 - Comunicações em HF entre Roménia e Portugal

Ao longo da Missão, o Módulo teve sempre presente o objetivo de melhorar as condições CSI da Força, quer em contexto operacional, quer em aquartelamento. Efetuou com frequência a manutenção e reparação de equipamentos de comunicações, dentro das suas capacidades, participou ativamente na dinamização de atividades de moral e bem-estar, esteve envolvido em atividades culturais romenas e ações de solidariedade.

O maior desafio encontrado durante a missão foi a interoperabilidade rádio com as Forças aliadas, sendo necessário que esta FND disponha de rádios credenciados pela NATO para a interligação com o escalão superior no decorrer dos exercícios.



As Transmissões na Missão de Treino Portuguesa na República da Guiné-Bissau

Sargento-Chefe Tm Guedes Pereira

Chefe da Equipa do Pilar de Transmissões Militares MTPT/RGB

Em dezembro de 2021 foram assinados acordos bilaterais entre Portugal e a República da Guiné-Bissau (RGB), pelos respetivos Ministros da Defesa Nacional.

Daqui resultou a constituição de um Grupo de Trabalho, sob a Liderança do TGen CEM CCOM Marco Serronha, para a implementação da Missão de Treino Portuguesa na RGB (MTPT/RGB). A referida missão visa garantir apoio técnico e formação, alicerçada em cinco pilares, sendo o desenvolvimento e manutenção da capacidade de Transmissões Militares um deles e cujo objetivo era providenciar apoio técnico ao desenvolvimento desta capacidade, através de uma bolsa de especialistas com competências em reparação de equipamentos (eletrónica), assim como o levantamento das redes rádio militares que se encontram inoperacionais.

Foi feita uma visita técnica à Guiné-Bissau entre 15 e 17 março de 2022, onde foram levantadas as necessidades para cumprir o objetivo da missão. Para representar o Pilar de Transmissões, foi nomeado o SCh Tm Francisco Pereira da DCI.



Figura 1 - Comitativa Portuguesa com as chefias militares Guineenses no EMGFA

Durante a visita ao EMGFA da Guiné-Bissau no Forte da Amura, as Entidades Guineenses salientaram a importância das comunicações para as Forças Armadas da Guiné-Bissau, assim como as dificuldades que estavam a atravessar. Não existiam Comunicações Militares entre nenhum dos Centros de Transmissões (CTm). A comunicação entre Unidades era feita com rádios “civis” Motorola e telemóveis. Os 23 CTm espalhados pelo território necessitavam de intervenções.

No Estado Maior do Exército, verificou-se que a oficina criada durante a Cooperação Técnico-militar (1994-2012) e que servia para reparação, manutenção e reabastecimento de material de transmissões estava inoperacional, não havendo a funcionar qualquer equipamento de medida, nem existência de ferramentas. Existia o edifício com as bancadas vazias, edifício esse que ficou danificado de forma irrecuperável, devido a uma forte tempestade pouco antes da chegada da equipa de Transmissões ao terreno.



Decorrente da visita, foi definida a missão da equipa:

- Levantamento das redes rádio militares que se encontram inoperacionais;
- Formar uma bolsa de especialistas com competências em reparação de equipamentos (eletrónica);
- Instalação de uma oficina de raiz (não previsto nos acordos de cooperação, mas imprescindível para o futuro) ;
- Apoio à Formação do 1º curso de Polícia Aérea (PA), ministrada aos militares Guineenses por militares da Força Aérea Portuguesa no âmbito da MTPT/RGB;
- Apoio na instalação de equipamentos para a melhoria das condições dos utentes da residência de Santa Luzia, da Cooperação no Domínio da Defesa (CDD) Portuguesa (fora do âmbito da Missão de Treino).

Para cumprir os objetivos da missão propôs-se:

- Nomeação de uma equipa composta por 3 Sargentos de Transmissões com a especialidade de Técnicos de Eletrónica e Equipamentos Rádio (TEER);
- Aquisição de material para equipar as bancadas da futura oficina;
- Módulos do P/PRC-425 para facilitar a reparação dos rádios;
- Baterias de 12V e fontes de alimentação para alimentar os equipamentos dos CTm, assim como diverso material elétrico.

Por proposta da DCI e Despacho de 08JUL22 SEXA ALM CEMGFA são nomeados para desempenhar a missão: SCh Tm Francisco Pereira da DCI; SAj Tm Telmo Patrício da DCI; SAj Tm João Brito do Destacamento da UAGME.

Com o apoio do Comando da Logística e Direção de Comunicações e Informação, conseguiu-se no Exército quase a totalidade dos materiais.

Para a futura oficina, reuniram-se equipamentos de medida, como um equipamento de teste CMS, geradores de sinais, osciloscópios, fontes de alimentação de bancada, frequencímetros, wattímetros, conjuntos de ferramentas de radiomontador, uma estação de soldadura/dessoldadura, módulos para o P/PRC-425 e diversos sobressalentes.

Para os Centros de Transmissões, reuniram-se antenas dipolo para HF, antenas VHF RC-292, fontes de alimentação, microtelefones e diverso material acessório, como cabo de RF, fichas e diverso material necessário à reinstalação e melhoramentos dos CTm.

Foi apenas necessário adquirir no mercado baterias de 12V e reguladores de corrente para os painéis solares.



Figura 2 - Equipa do Pilar de Transmissões Militares



A 01 de setembro de 2022 a equipa chega a Bissau e enquanto aguardava pela chegada de Portugal de uma viatura necessária aos deslocamentos, começaram a ser feitas visitas técnicas a todas as Unidades da zona de Bissau para fazer o levantamento das necessidades. Essas visitas eram feitas em movimentos apeados, ou fora do perímetro de Bissau, com o apoio das Entidades Guineenses em viatura militar. Foram visitados os CTm do EMFGFA, EME, EMMG, EMFA, Presidência da República, Guarda Nacional, Centro Instrução Cumeré, assim como as várias Brigadas e Regimentos pertencentes à Zona Militar Centro, com QG em Bissau.

Devido à inexistência de uma oficina de reparação, foi criada temporariamente uma na residência da CDD, onde foram testados e reparados vários rádios TR-28 e P/PRC-425, enquanto se dava formação “on job training” a 8 militares guineenses.



Figura 3 - Oficina improvisada na Residência da CDD

As Forças Armadas da Guiné-Bissau iniciaram na mesma altura a reconstrução de um edifício para a futura oficina. Durante este mês, foram feitos melhoramentos consideráveis nas instalações da residência da CDD, com a instalação de televisores e melhoramento da rede de internet. Mais tarde seria também instalado um sistema CCTV, melhorando assim a segurança.



Figura 4 - Entrega de material às Forças Armadas

A 08 de setembro é feita a entrega formal do material às Forças Armadas Guineenses, com a presença do Sr. Contra-Almirante Ramos Borges em representação do Chefe do Estado-Maior-General das Forças Armadas Portuguesas e do Brigadeiro-General Samuel Fernandes em representação do Chefe do Estado-Maior-General das Forças Armadas da Guiné-Bissau.

Com a chegada da viatura no início de outubro começam de imediato a ser feitas visitas técnicas ao interior do país, nomeadamente aos Comando das Zonas Militares Norte em Bula, Leste em Bambadinca e Sul em Buba. Foram feitas também visitas aos Batalhões e Companhias que compõem as Zonas, como Ingoré, Mansoa Farim, Bafatá, Gabú e Cufar para o levantamento das necessidades.

A fase seguinte foi a reparação e reestruturação dos CTm, numa luta contra o tempo até final da missão. Esses deslocamentos eram bastante demorados, devido às degradadas condições das estradas e, no caso de Farim, ter de utilizar uma jangada para atravessar o rio.



Figura 5 - Travessia do Rio Cacheu – Farim



Figura 6 - Visita ao Comando da Zona Militar Leste - Bambadinca

No final de outubro foi prestado apoio à equipa da Força Aérea Portuguesa que ministrava o 1º Curso de Polícia Aérea. Foi dada uma formação básica de Procedimentos Radiotelefónicos na Base Aérea de Bissalanca.



Figura 7 - Formação de Transmissões ao 1º Curso de Polícia Aérea



Figura 8 - Formadores e instruídos

No último dia de novembro é terminada a instalação da oficina. Foram criadas bancadas para reparação de rádios HF TR-28, bancada para P/PRC-425 e uma bancada com uma estação de soldadura/dessoldadura. Foi também criado um gabinete para o chefe, uma secretaria, uma sala de receção e entrega de material e um armazém de material de transmissões.



Figura 9 - Inauguração da Oficina, com breve explicação às Entidades



A inauguração contou com representantes do EMGFA PT, EMGFA RGB, EME RGB, do Sr Adido de Defesa PT, entre outra entidades e uma equipa de Reportagem da CMTV.

Aproveitando a equipa no terreno e a poucos dias do regresso a Portugal, em dezembro é pedido pelas chefias Guineenses o restabelecimento das comunicações militares com o arquipélago dos Bijagós, perdida há cerca de 3 anos. Devido à sua importância, foi assumido que estabeleceríamos a ligação. O meio de transporte foi uma lancha.



Figura 10 - Transporte para o Arquipélago do Bijagós



Figura 11 - Instalação do CTm de Bubaque

Resultados obtidos

Nos Centros de Transmissões:

- Foram reparados e reequipados 23 CTm, sendo ainda criados 2 de raiz, passando as FA da RGB a dispor de 25 CTm. As Unidades passaram a estar todas ligadas e a ter comunicações militares 24h/dia.;
- Cada CTm foi reforçado com mais um rádio, ficando em armazém e melhorando assim as suas capacidades;
- Foi restabelecida a ligação do Arquipélago dos Bijagós à Guiné continental, perdida há mais de 3 anos;
- Foram recuperados cerca de 50 rádios TR-28 e 20 P/PRC-425;
- Para a realização das intervenções aos Centros de Comunicações fora de Bissau, foram percorridos quase 4000 Km. A viagem mais longa foi a Cufar, cerca de 690 km e demorando 16h só em viagem.



Figura 12 - Reparação e remodelação dos CTm



Foi instalada uma oficina de manutenção, reparação e armazenamento de material de transmissões com:

- 2 bancadas com equipamento de teste e medida;
- Uma bancada com equipamento de soldadura e dessoldadura;
- Toda a ferramenta necessária;
- Condições de armazenamento;
- Módulos para substituição.



Figura 13 - Oficinas

Foram formados 8 militares Guineenses:

- Formação *on job training*;
- Análise a um equipamento rádio, com deteção, reparação e ajustes;
- Manuseamento dos aparelhos de medida.

Intervenção na Residência de Santa Luzia – CDD:

- Instalação de TV em todos os quartos;
- Instalação de TV na Casa do segurança;
- Melhoria da rede de Internet;
- Instalação de sistema de videovigilância CCTV.



Figura 14 - Instalação CCTV na Residência de Santa Luzia- CDD



Figura 15 - Instalação CCTV na Residência de Santa Luzia- CDD

Passados 109 dias da chegada à Guiné-Bissau, a equipa regressou a Portugal tendo recebido fortes elogios e agradecimentos das altas chefias Guineenses pelo reconhecimento do trabalho realizado. Também em Portugal foi reconhecido o trabalho realizado, ao que SEXA ALM CEMGFA definiu como “... uma obra notável” em entrevista à CMTV, dignificando a arma de Transmissões e o Exército.

los, “Estes que se tinham visto no papel tornaram-se na realidade dos factos, pois os militares de uma e outra fôrma”, escreveu António Silva Ribeiro. O chefe de gabinete deste primeiro curso é a instalação, em São-tiago, de uma sala de comando e controlo. “E, no topo, um aparelho da FA Angolense e da FA portuguesa. Agora estamos em condições de fazer alguma coisa. De fazer cumprir o lei”, afirma o general Filipe Ferreira, chefe da Força Armada Guiné-Bissau.

Toda a Central ligada

Uma “obra notável”, como descreve o almirante António Silva Ribeiro, está a ser realizada por uma equipa de Comunicações do Exército português, que percorre a Guiné-Bissau a ligar as várias, “recolhendo, ativando e reparando” a rede de comunicações que há meses estava inoperacional por falta de manutenção. “As comunicações militares estavam completamente degradadas, praticamente não existiam, e

pouco existiam a nível diário. Agora, os 25 centros, neste momento, têm comunicações 24 horas por dia, 7 dias por semana”, assegura o sargento-chefe Ferreira, da equipa portuguesa: três elementos que também montaram, em Bissau, uma oficina para formação de militares guineenses. “Para que não se deixem degradar nem voltem a cair as comunicações militares conforme estavam.” “Antes da guerra de 7 de junho [1998] tivemos cooperação, mas com muitos problemas que aqui tivemos de ter de existir. Agora retomamos esse acordo. Faz-nos recuperar materiais e equipamentos que estavam quase perdidos”, diz o general Paulo Namora, vice-chefe do Exército da Guiné-Bissau.

Ainda a receber a ajuda

A Ajuda Militar Brasileira chegou 140 toneladas de material escolar e equipamento de ensino a Bissau. “Com o dinheiro vamos a comprar, trazer o que poder porque aqui há muita coisa



Principais atividades realizadas pelo RTm durante o ano de 2023

Major Tm Sílvia Gomes

Chefe da Secção de Operações Informações e Segurança do RTm

Com o ano de 2023 regressou a tão aguardada normalidade, após três anos de restrições e contingências devido ao período pandémico. O dia 01 de janeiro de 2023 marcou o definitivo encerramento de portas a milhares de cidadãos, utentes do Serviço Nacional de Saúde, que durante um ano e meio se dirigiram ao Centro de Vacinação Covid do Agrupamento de Centros de Saúde Porto Ocidental, instalado neste Regimento de Transmissões (RTm).

O Batalhão de Transmissões e a Companhia de Guerra Eletrónica, encargo operacional do RTm, participaram, ao longo do ano de 2023, em cerca de 20 exercícios nacionais e nos exercícios internacionais V2CN (Espanha) e CWIX (Polónia), garantindo ainda o apoio ao aprontamento de Forças Nacionais Destacadas, bem como, à formação interna para a operação dos novos meios que estão a ser recebidos no âmbito dos Projetos de reequipamento de Guerra Eletrónica e Comunicações.

Relativamente à Formação, foram ministrados pelo Regimento um total de 450 dias úteis de formação (DUF), com 26 cursos e 349 militares e civis formados nas vertentes de Redes de Computadores, Sistemas de Informação, Comunicações Rádio e Guerra Eletrónica. No âmbito da oferta formativa da Formação Inicial e de Progressão na Carreira foram realizadas 2 edições da Formação Específica Inicial 17-Comunicações, com 47 militares, e 4 edições do Curso de Promoção a Cabo, com um total de 184 militares formados.



Figura 1 - Atividade da iniciativa "Alista-te por um Dia"

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 entreaajuda, a solidariedade e o espírito de equipa, sendo reconhecido, pela maioria das entidades, como valores deficitários às novas gerações.



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, sendo reconhecido, pela maioria das entidades, como valores deficitários às novas gerações.

O Centro de Divulgação do Dia da Defesa Nacional, sediado no RTm, recebeu a 19ª Edição durante 45 dias úteis, de 16 de janeiro a 21 de março. Compareceram 5930 jovens residentes nos concelhos do Porto, Maia, Matosinhos e Valongo. O Regimento participou de forma ativa através de exposições de capacidades na área das Comunicações e Sistemas de Informação Táticos e de Guerra Eletrónica.



Figura 2 - Atividade da iniciativa "Alista-te por um Dia"

No âmbito da iniciativa “Alista-te por um Dia”, inserida no Programa de Divulgação das Forças Armadas, cerca de 630 alunos do 4º ano das escolas do concelho de Matosinhos, visitaram o Regimento no mês de fevereiro, onde tiveram a oportunidade de experienciar várias atividades militares adaptadas à sua faixa etária, sendo as cerimónias do Hastear e do Arriar da Bandeira Nacional momentos marcantes para estas crianças. Paralelamente, o RTm contribuiu para a execução das iniciativas “Cidadania e as Forças Armadas”, com alunos do 9º ano, tendo sido efetuadas palestras a 35 turmas de 10 escolas do concelho de Matosinhos, e “Portugal e as Forças Armadas” com os alunos do 12º ano. Em abril foi a vez da Unidade acolher 14 alunos do município de Lousada que participaram na iniciativa “Militar por um dia”, desenvolvida pelo Exército. 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 carácter essencialmente prático de natureza militar, promovendo a sua identificação com as Forças Armadas.



Durante o ano transato, foram várias as cerimónias militares e visitas de entidades militares e civis ao RTm. De destacar a cerimónia de Tomada de Posse do Comandante do RTm, as comemorações do Dia da Arma e do Regimento de Transmissões, em 24 de março, e a visita do 2º Comandante da Brigada de Intervenção, por ocasião da sua Tomada de Posse.

O RTm 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.

Em 2023 comprovou-se, uma vez mais, a generosidade dos militares e funcionários da Unidade, pela forma voluntária, pronta e altruísta como participaram nas três iniciativas de recolha de dádivas de sangue que foram realizadas em colaboração com o Instituto Português do Sangue e da Transplantação.



Figura 3 - Dádiva de sangue

Embora todo o ano tenha sido pleno de desafios e de um permanente esforço para cumprir prontamente todas as missões e tarefas cometidas ao RTm, o período estival foi, uma vez mais, muito desafiante, numa altura em que o ano de 2023 era já considerado o mais quente em quase dois séculos. No âmbito do apoio à proteção e salvaguarda de pessoas e bens, O RTm participou, durante os meses de agosto, setembro e outubro, em diversas ações de vigilância dissuasora e de rescaldo e vigilância ativa, 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 56 patrulhas de vigilância e dissuasão, num total de 28 dias de empenhamento, com 3 militares empenhados em cada patrulha e 7206 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 empenhada uma secção em reforço do pelotão de rescaldo e vigilância ativa pós rescaldo do RC6, na região de Castelo Branco. Esta ação teve a duração de 48 horas de empenhamento, com 7 militares empenhados e 246 km percorridos.

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 1162 km percorridos na região de Mirandela.



Figura 4 - Comemorações do dia da Arma e do Regimento de Transmissões

Sendo o atual efetivo disponível cerca de 45% do efetivo previsto em Quadro Orgânico, o cabal cumprimento de todas as missões e tarefas que este Regimento recebeu foi alcançado mercê de um comando e controlo flexível e do inequívoco profissionalismo e dedicação de todos os militares e civis que, Sempre Melhor, souberam prontamente responder.



Figura 5 - Militar do RTm em patrulha de vigilância e dissuasão



Arma de Transmissões - Dados estatísticos relativos ao ano de 2023

Capitão Tm Luís Regada

Chefe da Secção de Pessoal do RTm , em suplência

Apesar das alterações da situação de pessoal serem, regra geral, do conhecimento de todos, é natural acompanharmos de forma mais atenta as alterações de situação dos camaradas da nossa Arma. O presente artigo reúne um conjunto de dados relativos a Oficiais e Sargentos do Quadro Permanente da Arma de Transmissões, que no ano de 2023 viram alterada a sua situação, nomeadamente no que diz respeito 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

(1) Quadro Especial de Transmissões

Posto	NIM	Nome
Ten	01296218	Ricardo Manuel Gonçalves Moura
Ten	11883118	Ana Maria Azinheiro Catarino
Ten	12894318	Gonçalo Miguel Oliveira Rocha
Ten	01893918	Carlos Filipe Vieira Gomes
Ten	08750118	Alexandre Yu Jin
Ten	05738717	André Manuel Miranda Gomes Pereira
Ten	10708318	Guilherme Rodrigues Lourenço
Ten	10783118	José Miguel Martinho Silva

b. Sargentos

(1) Quadro Especial de Transmissões

Neste ano os dois alunos que frequentavam o 50º CTSP TM, desistiram.



2. PROMOÇÕES

a. Oficiais

(1) Quadro Especial de Transmissões

Posto	NIM	Nome
Cor	23469291	Pedro Alexandre Coutinho dos Santos
Cor	26475393	Gustavo Alexandre Rodrigues de Mesquita Ferreira Gapo
Cor	08204589	João Manuel Fernandes Correia
TCor	15360099	Ângelo Miguel Lopes Silva
TCor	03972200	Luís Carlos Oliveira Mendes
Maj	17970505	Humberto Nélon Ribeiro da Costa
Maj	09194305	João Carlos Ferreira Monteiro
Cap	07990113	António Fernando Alves Carneiro
Cap	13821214	Ivo Fernando Fontes Linhas Guerra
Cap	16291614	André Filipe da Silva Ferreira
Cap	14540514	Hélder Figueiredo Reia
Cap	14035614	João Miguel Nobre Pinto
Cap	12067613	João Gabriel Vieira Félix

(2) Quadro Especial de Técnicos de Exploração de Transmissões

Posto	NIM	Nome
TCor	055471387	José Joaquim Fernandes Palhau

b. Sargentos

(1) Quadro Especial de Transmissões

Posto	NIM	Nome
SMor	15955487	Pedro Miguel de Oliveira Martins
SMor	02073687	Francisco dos Santos Alves do Rosário
SMor	04194987	João José Moreira Fernandes
SMor	19446087	José Francisco de Sousa Moreira
SMor	01663788	António Fernando Monteiro Teixeira
SMor	11755888	Leonardo de Sousa Diogo
SMor	13927087	Celestino Manuel Abreu da Costa Rios



SCh	06930391	Carla Cristina Palma dos Santos Monteiro
SCh	20682391	Almor José Matos Mota Ribeiro
SCh	25670091	José Carlos Almeida da Silva
SCh	01475190	Pedro Miguel Lopes de Oliveira
SCh	07756790	Túlio Miguel dos Santos Ferreira
SCh	35331892	José Carlos da Conceição Lourenço
SCh	17943392	António de Jesus Marçal
SCh	21944691	Mário César Colaço Arede
SCh	09163094	Duarte Filipe Gomes Gato
SCh	19945191	Nelson Pedro Paixão da Silva Moço
SCh	10875791	Vítor Avelino da Cruz
SCh	06896991	Jorge Miguel Cabrita Santos
SCh	01247992	Maria Gourete de Oliveira Salvador
SCh	09737093	António Alexandre da Silva Veloso
SCh	07614192	Fernanda Maria Martins da Rosa
SAj	06542603	Rui Duarte da Costa Macedo
SAj	03183395	Eustáquio Freitas Nunes
SAj	10528203	Luís Daniel Pinho Soares Pinto
SAj	09958805	Filipe Duarte da Costa Cunha
SAj	10862999	Hélder Renato Queirós da Costa
SAj	09879805	Márcia Ribeiro da Silva
SAj	13960306	José Carlos Ferreira da Silva
SAj	07149409	Hugo Emanuel Gonçalves Cardoso
SAj	03892702	Luís Filipe Jorge de Oliveira
SAj	10116702	Júlio Ricardo Moreira Sebastião
SAj	04282305	João Vasco Marinho de Brito
SAj	09377098	José Emanuel da Fonseca Silva
SAj	09517299	Válter José Pires da Silva
SAj	02243804	Dália Valentina Gouveia Reis Rodrigues
SAj	00392296	Marco Paulo Fernandes de Oliveira Neves
SAj	11832699	Fábio Roberto de Sousa Mendes Almeida
SAj	12113200	Bruno Miguel Rodrigues Cachucho
SAj	06797501	Bruno Ricardo Das Neves Maricato
SAj	13711805	Ruben Timóteo de Oliveira Durão
SAj	02704904	Ricardo Jorge de Magalhães Trigo



1Sarg	09489712	Filipe da Fonseca Sousa
1Sarg	15722916	Miguel Ângelo Ferreira da Silva
1Sarg	15235816	Diogo da Moita Pereira
1Sarg	06658717	Jorge Abraão Gonçalves do Espírito Santo
1Sarg	10213617	Bernardo Marques Pontes
1Sarg	06735211	João Tiago Simões Mota Faro
1Sarg	12930813	Tiago Alexandre da Silva Nunes

3. PASSAGEM À SITUAÇÃO DE RESERVA

a. Oficiais

Posto	NIM	QEsp	Nome
Cor	17649887	TM	Vítor Manuel Pires Terras
Cor	03179286	TM	Francisco António Veiga
Cor	18964189	TM	Carlos Alberto Garcia dos Reis
Cor	04087287	TM	João Carlos do Nascimento Nunes
Cor	17579089	TM	José Jaime Soares Pereira
TCor	18366287	TM	Carlos Manuel Sobral Pinto Nascimento
TCor	00353687	TEXPTM	Pedro Manuel da Silva Ferreira
TCor	05571387	TEXPTM	José Joaquim Fernandes Palhau

b. Sargentos

Posto	NIM	QEsp	Nome
SMor	05010186	TM	Carlos Craveiro Pereira
SMor	02073687	TM	Francisco dos Santos Alves do Rosário
SMor	19446087	TM	José Francisco de Sousa Moreira
SMor	01663788	TM	António Fernando Monteiro Teixeira
SMor	11755888	TM	Leonardo de Sousa Diogo
SMor	13927087	TM	Celestino Manuel Abreu da Costa Rios
SCh	01821987	TM	João Paulo Gaspar Vara
SCh	19767489	TM	Carlos Manuel de Oliveira Medina
SCh	04902988	TM	António Alberto Noronha Ribeiro
SCh	04716386	TM	Mário Luís Paquete Geraldo



4. PASSAGEM À SITUAÇÃO DE REFORMA

a. Oficiais

Posto	NIM	QEsp	Nome
Cor	06013881	TM	António Manuel Rosa Salvado
TCor	10585485	TM	João Manuel Marques Maia
TCor	04980383	TEXPTM	José Joaquim da Silveira Magalhães
TCor	12280778	TEXPTM	Manuel José da Silva Bastos
Maj	13693884	TEXPTM	Mário Jorge Alves da Silva

b. Sargentos

Posto	NIM	QEsp	Nome
SMor	04252784	TM	Mário António Rodrigues Correia Pereira
SMor	14227584	TM	José Carlos Alves
SMor	00685184	TM	Júlio César Gaspar Marçalo
SAj	03565482	TM	Hernâni Alexandre Leite da Silva Martins
SAj	14242587	TM	Adelino Manuel de Castanheira e Vale
SAj	02150282	TM	Mário José Ribeiro Duarte

5. ABATE AO QUADRO PERMANENTE

a. Oficiais

Posto	NIM	QEsp	Nome
Maj	11442101	TM	Luís Filipe Xavier Cavaco de Mendonça Dias
Maj	15506201	TM	Tiago Filipe Abreu Moura Guedes
Cap	18931911	TM	André Alves Silva
Cap	19650013	TM	Jorge Diogo Dias Abrantes Farinha
Cap	15177212	TM	David Filipe Rodrigues Lopes

b. Sargentos

Posto	NIM	QEsp	Nome
SAj	22030391	TM	José Luís Silva Elias
SAj	00780394	TM	Fernando Miguel Santos Oliveira Talhadas
SAj	05798500	TM	Ilídio Rafael de Almeida Amaral



6. OBITOS

a. Oficiais

Posto	NIM	QEsp	Nome	Data Falecimento
Cor	50972611	TM	Fernando Luís da Costa Ferreira	21Nov23
Cor	08751380	TM	Fernando Cunha dos Santos Pinto	14Ago23
TCor	04013266	TMANTM	Luís da Conceição Almeida Rocha	22Set23
Cap	50981411	TEXPTM	Mário José de Freitas Rodrigues	04Ago23
Cap	52112411	TEXPTM	José Pinheiro Almeida	27Out23
Cap	51212911	TEXPTM	António Augusto Santos Simões	06Ago23

b. Sargentos

Posto	NIM	QEsp	Nome	Data Falecimento
SMor	50250411	TM	Manuel António Martins Leal	24Dec23
SCh	50207711	TM	Manuel Fernandes Pimenta	25Jan23
SAj	50980711	TM	José Esperança Palma Pereira	14Jun23
SAj	39304058	TM	António Manuel Queijo	09Ago23
SAj	00694977	TM	António Nuno Coelho Rodrigues	07Jul23
1Sarg	51511411	TM	António Rodrigues Vilhena	21Ago23
1Sarg	35248956	TM	José Ricardo Martins	02Jan23



A Formação no Regimento de Transmissões

Major Tm Martingo Coelho

Chefe da Secção de Formação do RTm

O Regimento de Transmissões (RTm), como Polo de Formação da Escola das Armas (EA), tem a especificidade da formação na área de Comunicações e Sistemas de Informação (CSI), que é a base que sustenta o conhecimento técnico para o desempenho de funções dos Quadros que trabalham nesta área. A constante evolução tecnológica, associada ao aumento da complexidade dos Sistemas de Informação e Comunicações, que apoiam o Sistema de Forças Nacional (SFN), implicam uma atualização frequente da formação de CSI, para uma adequada preparação dos militares e civis para a operação, configuração e gestão dos respetivos sistemas e equipamentos.



Figura 1 – Curso IT-Essentials da Academia Cisco no RTm

Neste sentido, a implementação da Academia Cisco e da Academia Microsoft, no RTm, permitiram que se passasse a ministrar 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.



Figura 2 – Curso MTA-Windows Server da Academia Microsoft no RTm



A oferta formativa deste Regimento encontra-se organizada em diferentes áreas: Redes de Comunicações (Academia Cisco), Aplicações e Sistemas de Informação (Academia Microsoft), Comunicações Rádio e C2, Guerra Eletrónica (GE), Material e Segurança Cripto para Praças, ministrando ainda cursos de “Formação Específica Inicial (FEI) 017 – Comunicações” e cursos de Promoção a Cabo.

O Regimento de Transmissões é um polo de formação atípico pela grande quantidade de cursos ministrados por ano. Durante o último ano de 2023, foram ministrados os seguintes cursos/ formações do Plano de formação Anual (PFA):

• IT-ESSENTIALS ○ 1.ª Edição de 23Fev23 a 22Mar23 ○ 2.ª Edição de 26Abr23 a 24Mai23 ○ 3.ª Edição de 16Out23 a 13Nov23	• CISCO CERTIFIED NETWORK ASSOCIATE - ROUTING&SWITCHING ○ 1.ª Edição de 27Fev23 a 23Jun23 ○ 2.ª Edição de 03Mai23 a 27Jul23
• CISCO CERTIFIED NETWORK ASSOCIATE – CYBERSECURITY OPERATIONS ○ De 16Nov23 a 15Dec23	• MICROSOFT TECHNOLOGY ASSOCIATE -WINDOWS SERVER ○ 1.ª Edição de 23Mar23 a 02Mai23 ○ 2.ª Edição de 25Mai23 a 23Jun23 ○ 3.ª Edição de 14Nov23 a 13Dec23
• MICROSOFT OFFICE SPECIALIST ○ 1.ª Edição de 16Jan23 a 10Fev23 ○ 2.ª Edição de 25Set23 a 24Out23	• MATERIAL E SEGURANÇA CRIPTO – PRAÇAS ○ 1.ª Edição de 13Fev23 a 17Fev23 ○ 2.ª Edição de 03Jul23 a 07Jul23 ○ 3.ª Edição de 11Set23 a 15Set23 ○ 4.ª Edição de 06Nov23 a 10Nov23
• OPERAÇÃO DO SISTEMA P/525 ○ 1.ª Edição de 09Jan23 a 13Jan2 ○ 2.ª Edição de 13Fev23 a 17Fev23 ○ 3.ª Edição de 17Abr23 a 21Abr23 ○ 4.ª Edição de 10Jul23 a 14Jul23 ○ 5.ª Edição de 20Nov23 a 24Nov23 ○ 6.ª Edição de 18Dec23 a 22Dec23	• CONFIGURAÇÃO E GESTÃO DO SISTEMA P/525 ○ 1.ª Edição de 16Jan23 a 27Jan23 ○ 2.ª Edição de 04Set23 a 15Set23 ○ 3.ª Edição de 27Nov23 a 12Dec23



• FUNDAMENTOS E ESTRUTURA DE GUERRA ELETRÓNICA ○ De 06Fev23 a 10Fev23	• OPERAÇÕES DE GUERRA ELETRÓNICA ○ De 03Out23 a 30Nov23
• FORMAÇÃO ESPECÍFICA INICIAL (FEI) 017 – COMUNICAÇÕES ○ 1.ª Edição de 06Mar23 a 31Mar23 ○ 2.ª Edição de 02Out23 a 31Out23	• CURSO DE PROMOÇÃO A CABO ○ 1.ª Edição de 06Fev23 a 17Fev23 ○ 2.ª Edição de 15Mai23 a 26Mai23 ○ 3.ª Edição de 04Set23 a 15Set23 ○ 4.ª Edição de 06Nov23 a 17Nov23

O RTm tem disponibilizado este tipo de formação certificada e de qualidade reconhecida a militares e civis dos três ramos das Forças Armadas, Forças de Segurança, militares de outros países, bem como a entidades civis. Destacam-se os cursos ministrados a militares das Forças Armadas de Cabo Verde (cooperação no domínio da Defesa/Cooperação técnico militar com a República de Cabo Verde), militares de países estrangeiros no âmbito da Iniciativa 5+5 Defesa (na 1.ª Edição do curso CCNA R&S de 2023, participaram militares da Líbia, Malta, Espanha, Argélia e Tunísia). De destacar ainda o curso CCNA-CyberOps, que tem tido a presença assídua de militares do Centro de Ciberdefesa do Estado-Maior General das Forças Armadas (EMGFA).

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 pelo Regimento de Transmissões.



Figura 3 - Curso CCNA-R&S da Academia Cisco no RTm



De realçar ainda a organização e realização do primeiro curso de Operações de Guerra Eletrónica que decorreu no Regimento de Transmissões, no período de 03Out23 a 30Nov23, no âmbito do PFA de 2023. Este curso de especialização, com a duração de 40 (quarenta) dias úteis de formação, visou habilitar os formandos com conhecimentos técnicos necessários para a execução de tarefas relacionadas com o planeamento e condução de operações de Guerra Eletrónica em apoio a Operações Militares Terrestres ou Conjuntas, bem como os conhecimentos necessários para integrarem uma Célula de Coordenação de Guerra Eletrónica.



Figura 4 – Ação de Vigilância Eletrónica

A vasta oferta formativa e a reconhecida qualidade da mesma, deve-se sobretudo ao grande esforço dos militares que prestam serviço como formadores nas diferentes áreas de formação deste Regimento, bem como pela obtenção de sinergias entre a formação e emprego operacional, consequente das inerentes competências do Regimento de Transmissões.

No entanto, apesar do reconhecimento comprovado da qualidade da formação ministrada, a volatilidade existente nas funções dos militares do Exército, dificulta a estabilidade necessária para a preparação e atualização de formações na área das CSI. A elevada componente técnica dos cursos ministrados, bem como a crescente oferta formativa nesta área, impõe a existência de um Quadro Orgânico na Secção de Formação com recursos humanos efetivos superiores aos existentes atualmente, de forma a garantir a manutenção das valências anteriormente referidas, bem como a expansão da oferta formativa para novas tecnologias.



Figura 5 - Curso de Operações de Guerra Eletrónica



1.º Curso de Operações de Guerra Eletrónica



Major Tm Humberto Costa
Chefe do Centro de Guerra
Eletrónica

Capitão Tm Miguel Gonçalves
Comandante de Companhia
Guerra Eletrónica

A Capacidade Terrestre de Guerra Eletrónica (CTGE) é a capacidade militar responsável por executar Operações no Espectro Eletromagnético, assegurando o seu domínio em prol das Operações Militares Terrestres (OPMILTER) existentes ou emergentes. Os conflitos contemporâneos, especialmente o da Ucrânia-Rússia, têm vindo a re-comprovar a importância tática, operacional e até mesmo estratégica da CTGE. Este envolvimento em OPMILTER reais, contribuindo simultaneamente para várias funções de combate (Informações, Fogos, Proteção da Força), estabelece a CTGE como um *enabler* multidomínio importantíssimo que só é capaz de funcionar efetivamente através da aplicação de tecnologia de ponta e militares extremamente bem formados e treinados. Para que a CTGE possa atingir um estado operacional no qual está considerada capaz de ser empenhada em OPMILTER reais deve ter existido a montante o seu completo desenvolvimento. É por isso que o processo de edificação de qualquer Capacidade Militar assenta em vários Vetores de Desenvolvimento de Capacidade, sendo a Formação e Liderança um vetor fulcral.



Figura 1 - Militar da Companhia de Guerra Eletrónica numa ação de vigilância eletrónica

A Companhia de Guerra Eletrónica (CompGE) é o único Elemento da Componente Operacional do Sistema de Forças responsável pela operacionalização da CTGE o que a torna excecionalmente singular e valiosa em termos operacionais. No entanto, devido à estagnação do investimento financeiro e de capital humano, o conhecimento interno acumulado foi reduzido ao mínimo. Esta situação conduziu a uma extrema desatualização da formação avançada em Guerra Eletrónica (GE) e, por consequência, à inexistência de Operadores de GE, de Analistas de Sinais e de Planeadores de Operações de GE capazes de integrar Unidades Táticas de GE ou Células de Coordenação de GE.



Assim o Exército, impulsionado pela necessidade de formar os futuros quadros da CompGE, aliado ao recente investimento em sede da Lei de Programação de Programação Militar decidiu reedificar a sua CTGE através do Projeto de Meios de Guerra Eletrónica. Desta forma, foi possível apostar na recuperação parcial do conhecimento técnico e operacional perdido.

Este desiderato foi atingido, com o desenvolvimento e realização do 1.º Curso de Operações de Guerra Eletrónica (COGE), de 03Out23 a 30Nov23, no Regimento de Transmissões, inserido no Plano de formação Anual. O COGE visou habilitar os formandos com os conhecimentos técnicos necessários para a execução de tarefas relacionadas com o planeamento e condução de Operações de Guerra Eletrónica, em apoio a Operações Militares Terrestres ou Conjuntas, bem como com os conhecimentos necessários para integrarem uma Célula de Coordenação de Guerra Eletrónica.

A preparação, construção e organização do curso foi inspirada nos antigos Cursos de GE e de Operadores de GE, Curso de Engenharia Eletrotécnica da Academia Militar, o Curso de Fundamentos de GE da Força Aérea, o Curso de Aperfeiçoamento de Oficiais em GE da Marinha e no NATO *Electronic Warfare Operational Planning Course*, da NATO *School Oberammergau*, direcionada para a realização de Operações de GE Terrestres.

Esta formação avançada em GE é composta por 40 DUF, perfazendo 280 TF e é dirigida a Oficiais e Sargentos da Arma de Transmissões do Exército ou equivalente nas Forças Armadas e Forças e Serviços de Segurança. O seu currículo está dividido em 7 Módulos de Formação:

1. Módulo A - Teoria de Telecomunicações;
2. Módulo B - Medidas de Apoio Eletrónico sobre Comunicações Táticas;
3. Módulo C - Análise de Sinais de Comunicações Táticas / Tactical COMINT;
4. Módulo D - Contra Medidas Eletrónicas sobre Comunicações Táticas;
5. Módulo E - Tática & Planeamento de Operações de Guerra Eletrónica;
6. Módulo F – Simulação de Sistemas de Guerra Eletrónica;
7. Módulo G – Condução de Operações de Guerra Eletrónica.

Frequentaram esta primeira edição 6 militares de entre os quais 2 oficiais e 4 sargentos, todos do RTm e em desempenho de funções no Centro de Guerra Eletrónica (CGE) e na Companhia de Guerra Eletrónica (CompGE).



Figura 2 - Militares que concluíram com aproveitamento o 1º Curso de Operações de Guerra Eletrónica 2023



Atendendo que os formandos têm necessariamente bases teóricas distintas, foi essencial a superação do desafiante Módulo A. Este módulo permitiu um nivelamento teórico sobre a teoria de telecomunicações entre todos os formandos. Os módulos B a D entraram em profundidade naquilo que é o *Core Business* técnico associado às Medidas de Guerra Eletrónica, permitindo aos formandos entender, em detalhe, o racional técnico que envolve cada uma das tarefas associadas às Medidas de GE. Uma vez consolidadas as componentes teórica e técnica, o curso avançou para a componente tática e de planeamento de Operações de GE, conteúdo essencial para todos os militares do CGE e da CompGE no cabal desempenho das suas funções. A componente tática e de planeamento permitiu analisar em detalhe o conceito de emprego tático de uma Unidade de GE de Escalão Companhia, com todas as suas valências, nos mais variados tipos de operações militares; permitiu elucidar os formandos sobre todos os passos do Processo de Decisão Militar (PDM), incidindo particularmente, em cada passo, para as necessárias preocupações e adaptações, tendo em vista o planeamento de uma Operação de Guerra Eletrónica.

Tirando partido do Sistema de Simulação de GE existente na CompGE os formandos tiveram a adequada formação na configuração e operação do sistema, permitindo o treino dos Operadores de GE, numa plataforma com a mesma interface que os Radiogoniómetros Digitais Táticos (RADITAC), mas em ambiente simulado. Neste módulo os formandos tiveram ainda formação orientada para a instalação e operação dos RADITAC e dos sistemas de Análise de Sinais.

Por último, e por forma a validar em contexto prático todo o conhecimento adquirido, o Módulo G baseou-se na realização de um Exercício da tipologia LIVEX, onde os formandos materializaram o planeamento realizado no Módulo E. Este exercício decorreu na Serra de Valongo durante 1 DUF, durante o qual os formandos, com recurso aos equipamentos existentes na CompGE, tiveram a oportunidade de colocar em prática os conhecimentos técnico-táticos necessários para a condução de uma pequena Operação de Guerra Eletrónica.



Figura 3 - Equipa de Guerra Eletrónica em operação durante o Exercício final do COGE



Esta primeira edição do COGE, marca o regresso de uma formação avançada de GE, que se alinha temporalmente com o atual esforço realizado pelo Exército na edificação da sua Capacidade de Guerra Eletrónica Terrestre, tecnologicamente adequada aos atuais desafios. No entanto é necessário ter presente que a CTGE evolui constantemente em tempo de paz e exponencialmente em tempo de conflito e é considerada uma matéria crítica e sensível e por si só bastante reservada. Por isso, as diferentes nações, que primam por manter uma CTGE atualizada, tendem a não partilhar informação relacionada com a sua CTGE com terceiros, mesmo que aliados. Veja-se novamente o caso do conflito Ucrânia-Rússia onde se sabe claramente que existem constantes Operações de Guerra Eletrónica, mas que são encobertas o mais possível. Afinal a informação é o ativo mais importante num conflito e ninguém quer abrir mão dela.



Figura 4 – Militar Ucrâniano a operar um equipamento de GE (Plastun-RP3000).

Fonte: <https://euro-sd.com/2023/09/articles/33980/silent-struggle-accounts-from-the-frontlines-of-ukraines-electronic-war/>

Assim, é necessário repensar o modelo de formação na área de GE para que, a par das formações em Operações no Ciberespaço e em Redes e Sistemas de Computadores, se possa introduzir currículos técnicos civis, uma vez que a indústria e a academia são as principais geradoras da tecnologia de ponta e conhecimento técnico em que assenta a GE.

Vemos onde a vista não alcança.



Produção de Energia através de um Sensor de Movimentos acoplado a um Íman Permanente

Sargento-Chefe Tm Mário Geraldo
Reserva

Nos dias de hoje, as comunicações são primordiais para o soldado. É essencial receber e transmitir instruções a vários níveis para uma tomada de decisão rápida e precisa. A resposta a estas solicitações só foi possível, devido à evolução tecnológica dos equipamentos. Associado a isso, devido a uma maior necessidade de energia, o soldado tem de transportar no colete tático cada vez mais baterias. Estes equipamentos são alimentados pelas suas próprias baterias, que têm tensões de alimentação e autonomias diferentes, o que obriga a uma criteriosa utilização. Quando estas se esgotam têm de ser trocadas por outras com carga, obrigando o soldado a levar consigo mais baterias e, consequentemente, mais peso.



Figura 1 – Soldados em deslocamento



Figura 2 – Colete tático



Figura 3 – Soldado com colete

Perante o desafio da evolução tecnológica dos equipamentos, a ideia passa por centralizar a gestão e produção de energia num único módulo, com várias interfaces de saída para alimentar os equipamentos necessários. Os blocos integrantes no módulo são independentes, de modo a permitir que os processos sejam otimizados, tenham margem de evolução e que seja possível em qualquer momento integrar novas tecnologias.

O conceito principal é aproveitar os movimentos do soldado para produzir a energia necessária para os equipamentos que transporta. Para a sua implementação elaborou o organigrama da figura 4. A linha de blocos a cor verde representa as fases para a sua concretização e a linha a cor de laranja representa a sua materialização.

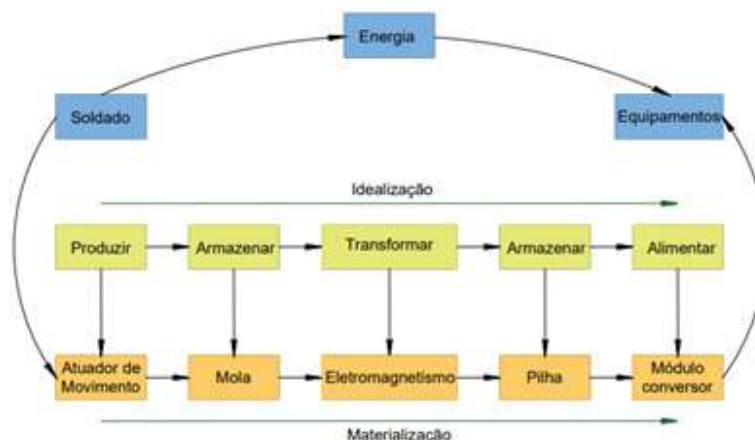


Figura 4 – Organigrama da Ideia



O produto final é o Módulo Integrador de Energia (MIE), que apresento na figura 5.

Legenda:

MIE – Módulo Integrador de Energia;

MGP – Módulo Gestão Potência;

MGE – Módulo Gerador de Energia;

AM – Atuador de Movimento.

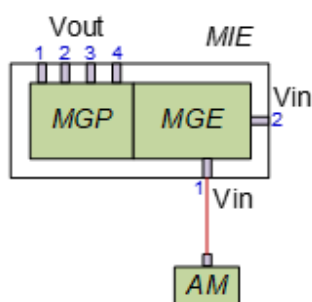


Figura 5 – Esquema do MIE



Figura 6 – Esquema do MIE

Pela análise biomecânica do corpo humano, verifica-se que os membros são a parte que mais energia cinética produz. Foi decidido projetar um Atuador de Movimento (AM) que colocado numa articulação lateral numa joelheira, consegue extrair a energia cinética dos movimentos de contração e distensão da perna. Esses movimentos desenvolvem ângulos com uma amplitude de 0 a 130 graus, figura 7.



Figura 7 – Soldado em movimento



Figura 8 – Articulação de poliuretano de alta resistência

O funcionamento do AM baseia-se numa válvula pneumática de alavanca rotativa, que é acionada pelos movimentos de contração e distensão da perna que criam pressão no circuito pneumático e originam uma força. A articulação é feita de poliuretano de alta resistência, material utilizado na indústria ortopédica para o fabrico de próteses e que poderá ser inserida nas calças. A válvula pneumática de alavanca rotativa, é produzida pela empresa AirTAC, modelo 4HV2-06, com as dimensões 62x62x84 mm e pesa 200 g. A força exercida pela válvula através do ar comprimido no circuito pneumático, vai movimentar um cilindro rotativo num sentido.



Figura 9 – Articulação lateral para o joelho

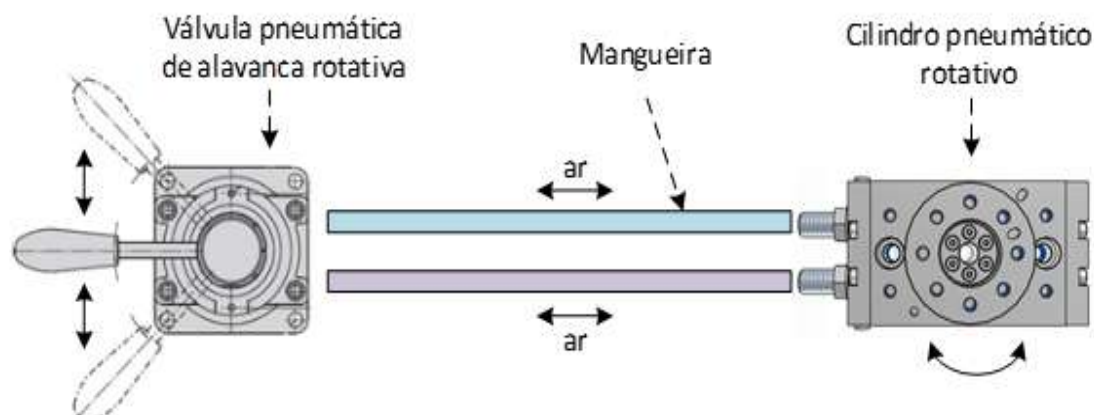


Figura 10 –Circuito pneumático

O cilindro escolhido é fabricado pela AirTAC, modelo HRQ2, com dimensões 32x76x28 mm e pesa 230 g. As mangueiras são do tipo Multi-Air à prova de dobras o que permite a passagem do ar mesmo com a mangueira torcida. Os conectores pneumáticos são de qualidade superior, com retentor de tubo em aço inoxidável. O movimento de rotação do cilindro, vai comprimir uma mola de tração e carregá-la com energia potencial elástica, figura 11.

A lei de Hooke estabelece que quando uma mola é deformada por uma força externa, uma força elástica restauradora passa a ser exercida na mesma direção, mas em sentido oposto. Essa força é diretamente proporcional à sua deformação. A mola de tração escolhida é da marca SPIROFLEX modelo 9S, em aço, esta mola tem uma energia elástica de distensão de 50 voltas.



Baseado no princípio de funcionamento do relógio mecânico, projetou-se um sistema com duas molas de tração, que vão ser comprimidas pelo movimento rotativo do cilindro.

As molas vão ser carregadas uma de cada vez, quando uma atingir a carga máxima, um mecanismo faz a comutação para a outra. Assim uma das molas está a ser comprimida, a outra através da sua distensão, desenvolve trabalho e coloca o sistema a funcionar, figura 12.

O cilindro rotativo faz rodar uma roda de carregamento. A roda de carregamento ao comprimir uma das molas, carrega-a com energia potencial elástica. Quando a mola atingir a carga máxima um mecanismo comuta para a outra. Enquanto uma das molas está a receber carga, a outra através da sua distensão põe o sistema a funcionar. O objetivo é ter uma roda a girar a uma velocidade de 1 volta por segundo.

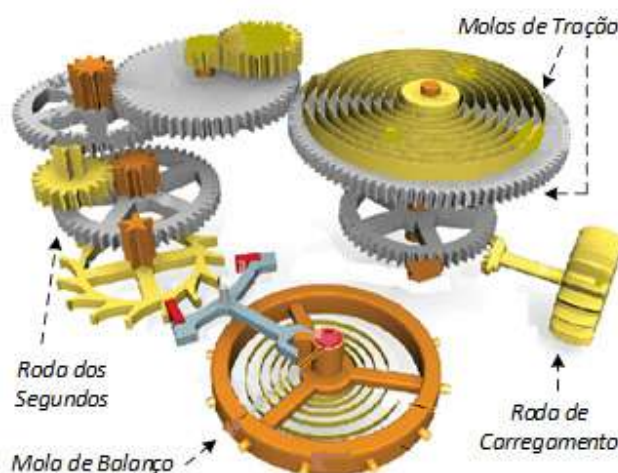


Figura 12 – Sistema mecânico de carregamento das molas



Na roda que está a girar a uma velocidade de 1 volta/s, fixa-se um mecanismo de “Roda-Manivela”, com um êmbolo na extremidade, figura 13.

O mecanismo Roda-Manivela converte o movimento circular em movimento retilíneo; Transmite esse movimento, através de um êmbolo, à parte eletromagnética do sistema.

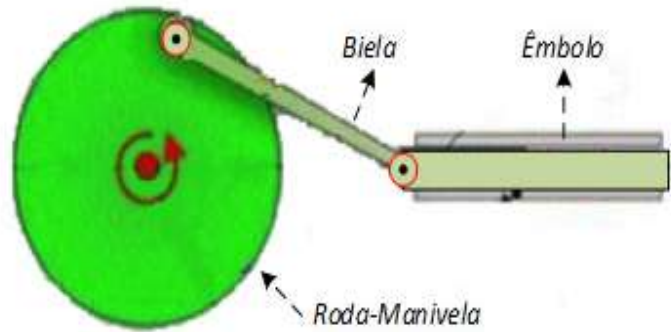


Figura 13 – Mecanismo manivela-bielao

O sistema eletromagnético é composto por Ímanes permanentes e um Solenoide.

O Íman Permanente escolhido é de Neodímio N35 (NdFeB) composto por neodímio, ferro e boro, figura 14.



Figura 14 – Íman de Neodímio

Características:

Dext=40 mm, Dint=10 mm, Altura = 5 mm, Peso = 44 g;

Campo magnético (B) = 313 mT;

Fluxo (Φ) = 0,000313 Wb;

Projetou-se um Solenoide com as dimensões de (LxAxD) 100x30x40 mm, com 12 camadas, cada camada com 40 espiras, totalizando 480 espiras bobinadas com fio de cobre esmaltado AWG30 (2,5 mm).

As linhas do campo magnético incidem perpendicularmente na área do Solenoide, cujo valor é, $\text{Área} = \pi r^2 = 3,14 \times 0,05^2 = 0,00785 \text{ m}^2$, figura 15

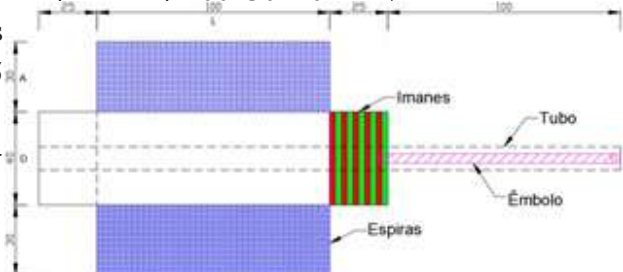


Figura 15 – Dimensões do Solenoide

O Íman produz um fluxo magnético de $\vec{\Phi} = B \times A \times \cos \theta = 0,313 \times 0,00785 \times 1 = 0,0025 \text{ Wb}$. Associando 5 ímanes fica-se com um fluxo de $\vec{\Phi} = 0,0125 \text{ Wb}$.

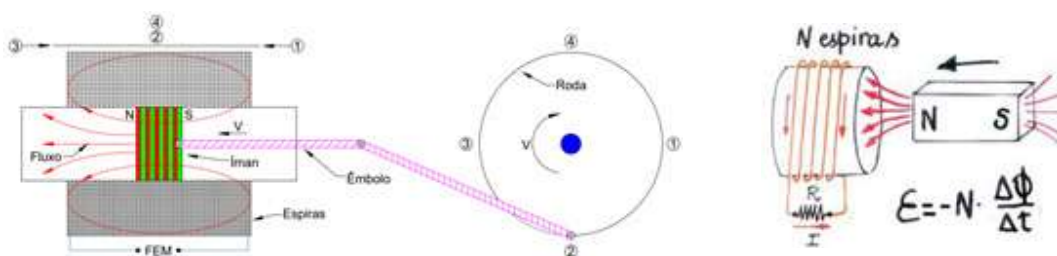


Figura 16 – Sistema eletromagnético

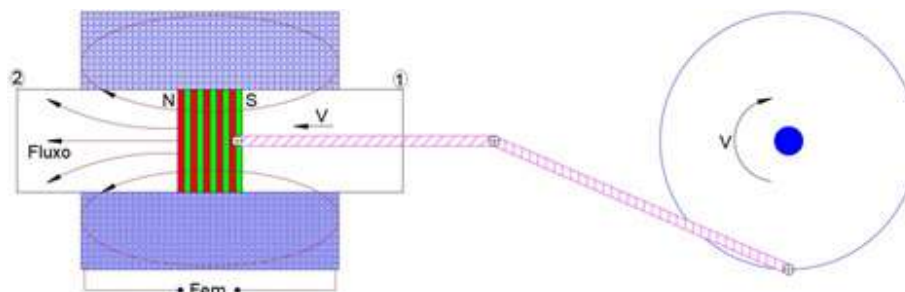


Figura 17 – Linhas do campo magnético impostas pelo Ímã

O movimento de rotação da roda (1 volta/s) faz com que o Ímã se mova no interior do Solenoide a uma velocidade de 200 mm/s. Este movimento origina uma variação de fluxo magnético entre os valores mínimo (0 Wb) e máximo (0,0125 Wb), a uma cadência de 2 vezes/s. Esta variação de fluxo vai produzir uma corrente induzida nas espiras do solenoide, que por sua vez, vai originar uma Força Eletromotriz (Fem) aos terminais da bobina, com o valor de 12 V.

$$\begin{aligned} F_{em} &= N \times \frac{\delta \Phi}{\delta t} = N \times \frac{\Phi_1 - \Phi_2}{t_1 - t_2} = \\ &= 480 \times \frac{0 - 0,0125}{0 - 0,5} = 12 \text{ V} \end{aligned}$$

Para gerir a distribuição da energia para os equipamentos, projetou-se um Módulo de Gestão de Potências (MGP), que vai fazer a transição energética entre as entradas e as saídas. O MGP tem incorporada uma bateria de íões de lítio, que funciona como uma almofada, com a finalidade de receber a energia das entradas e disponibiliza-a nas saídas.

A bateria escolhida é do tipo LI-PO-3s da SIGMA. Com uma tensão de 11,1 V, capacidade 2200 mAh, dimensões 105x35x24 mm e com o peso de 179 g.

A principal função do MGP, é regular e controlar as saídas (Vout) e entradas (Vin). Utiliza tecnologia MPPT “Maximum Power Point Tracking” para tirar o máximo rendimento das fontes de energia e nas saídas manter as tensões de alimentação constantes e estáveis.

Na entrada Vin1 liga o MGP, a entrada Vin2 é para ligar um painel solar, uma turbina eólica ou uma tomada de energia existente nas viaturas. É destinada para alimentar o sistema, quando o soldado está numa situação em que se encontra parado.



Figura 18 – Bateria alta densidade



O MGP é do tipo “System on-Chip” (SoC).

Um SoC é um conjunto de circuitos integrados num único “chip”, onde existem blocos funcionais diferentes e autónomos.

Legenda:

Vin – Entrada;

Vout – Saída;

MPPT - Maximum Power Point Tracking

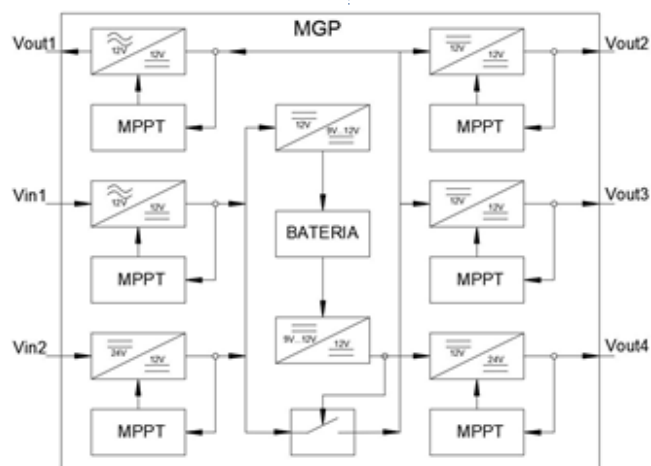


Figura 19 – Esquema de blocos do MGP

O resultado esperado é um Módulo Integrador de Energia versátil, escalável, com uma potência de 30 W e um peso abaixo dos 2 Kg. Através da substituição do Atuador de Movimento é possível gerar energia a partir de outra parte do corpo. O Módulo de Gestão de Potências está preparado para receber energia de qualquer fonte, eólica, solar, pilha de hidrogénio ou simplesmente elétrica.

A tecnologia proposta é implementada em muitos sistemas, que estão a funcionar com resultados comprovados. A ideia está fundamentada em conceitos teóricos e cálculos matemáticos. O material para a sua implementação está identificado, sendo que o projeto e fabrico das peças mais exigentes, tem de ser feito por empresas especializadas.

A próxima fase é a validação funcional em laboratório. É natural que nesta fase o sistema apresentado passe por algumas modificações e ajustes, principalmente ao nível das dimensões e peso.

As mais valias que se obtêm com a sua implementação da ideia são:

1. Não estar dependente de um único método para alimentar os equipamentos;
2. Criar um sistema autónomo, que só dependente do atuador e da forma de movimento;
3. Criar um módulo dinâmico, adaptável a todas as fontes de energia emergentes;
4. Sistema que pode ser adaptado para alimentar os equipamentos instalados nas viaturas, nos centros de comunicações e nas estações de transmissão.

Como dizia Lavoisier, *Nada se cria e nada se perde, tudo se transforma.*



Extensão da rede RED a escalões táticos

Alferes-Aluno Tm Daniel Almeida

TPO Transmissões

Resumo - Nas operações militares modernas, a comunicação segura e a troca de dados desempenham um papel fundamental para garantir o êxito das operações militares. Esta tese apresenta uma exploração da viabilidade de alargar os domínios classificados às unidades táticas inferiores, uma vez que a quantidade de informação a que os soldados têm acesso está a aumentar. O estudo está estruturado em três fases principais. Uma análise da literatura académica fornece os conhecimentos fundamentais sobre comunicações seguras e redes militares. Em seguida, foi realizado um trabalho de campo para reunir conhecimentos e requisitos do mundo real essenciais para a extensão de domínios classificados a unidades táticas inferiores. Por fim, é utilizada uma emulação de rede tática para simular as condições e os condicionais das redes militares operacionais. Isto permite uma avaliação prática do potencial de integração da cifragem e dos canais seguros em redes táticas com limitações de largura de banda, utilizando máquinas de cifra. Os resultados da emulação revelam que, embora a adição de encriptação seja efetivamente possível, é essencial reconhecer as limitações inerentes a estas redes. À medida que descemos na hierarquia da rede, a necessidade de uma encriptação leve torna-se cada vez mais pronunciada.

Introdução

Num cenário tecnológico em constante evolução, a comunicação militar segura e eficiente é vital. As redes táticas são essenciais na guerra moderna, enfrentando desafios como terrenos acidentados e ameaças à segurança.

O principal objetivo deste trabalho é expandir o domínio de segurança de uma rede tática militar, tendo em conta a existência de dispositivos de cifragem de baixo custo e leves, mas ainda assim acreditados. Os requisitos deste trabalho são avaliar se a utilização de máquinas de cifra aos mais baixos escalões, ainda mantém o desempenho da rede existente e se não há impacto na experiência do utilizador.

Estado da arte

Redes táticas heterogéneas

A cooperação efetiva em operações militares depende da colaboração entre nações. A NATO, reconhecendo este facto, criou a *Federated Mission Networking* (FMN) em resposta à natureza evolutiva da guerra moderna. A FMN funciona como um sistema em tempo real que permite aos países membros da NATO partilhar informações e recursos, melhorando a sua resposta coletiva a crises e emergências. Estudos recentes do grupo de investigação IST-124 da NATO revelam que as redes de nível tático inferior são diversas, empregando várias tecnologias de transmissão de rádio com diferenças na largura de banda, frequência e outros fatores. Esta diversidade coloca desafios como a variação de conectividade, atrasos, taxas de erro de bit elevadas e a necessidade de os nós operarem em silêncio de rádio atrás das linhas inimigas, tal como descrito em investigação recente sobre estratégias de encaminhamento tático [1]. Os rádios nos nós, podem ter ou não capacidade de encaminhamento, o que os torna rádios de camada 3 ou de camada 2, respetivamente. Os dispositivos criptográficos podem ser adicionados fora dos rádios ou construídos dentro deles.



Protected Core Networking (PCN): A PCN tem por objetivo criar uma infraestrutura militar de transporte IP segura e versátil. Ligando diversos segmentos de redes nacionais para formar uma rede de base mundial. A PCN dá ênfase à segurança e à qualidade do serviço, estando atualmente a ser objeto de normalização pela NATO como o STANAG 5637.

A PCN utiliza várias classes de serviços de rede para dar resposta aos requisitos de desempenho e segurança. Apresenta capacidades avançadas de conhecimento, gestão e controlo. A estrutura da rede está representada na Figura 1.

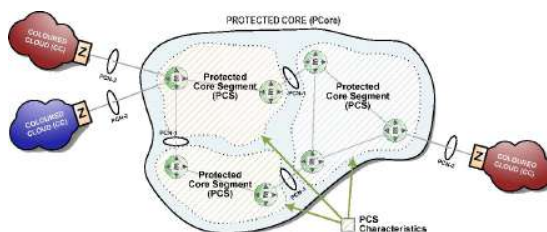


Figura 1 - Protected Core Network

A PCN inclui *Coloured Clouds (CC)* que se ligam a uma entidade central denominada *Protected Core*, que consiste em múltiplos segmentos, formando uma federação colaborativa. Os segmentos estão em conformidade com os princípios da PCN e interligam-se através de nós E na interface PCN-1 [2].

O *Protected Core* funciona como uma rede de transporte, com os utilizadores finais a ligarem-se através de CCs. O isolamento criptográfico garante a comunicação apenas entre CCs da mesma cor, denotando domínios de segurança específicos. Os nós que se ligam através de interfaces PCN-1 ou PCN-2 são submetidos a autenticação para segurança e integridade da rede.

Segurança em Redes Táticas

As proteções criptográficas podem ser introduzidas a vários níveis na camada OSI e podem ser aplicadas por um ou vários nós da rede. Estas salvaguardas podem ser colocadas no anfitrião final de origem, na infraestrutura de rede ou num rádio acedido através de uma rede encaminhada. Para simplificar, assume-se que todos os rádios são de nível 3.

Proteção ao nível da aplicação: A proteção ao nível da aplicação inclui qualquer tipo de proteção localizada, camada de rede ou superior. Consiste em mecanismos de proteção da camada de aplicação, bem como em IPSec ou TLS implementados no anfitrião. Ao utilizar o IPSec no anfitrião final para a proteção ao nível da aplicação, são necessárias menos despesas gerais quando se utiliza o modo de transporte em vez do modo de túnel.

Algumas vantagens da proteção ao nível da aplicação são o facto de a carga útil do utilizador estar verdadeiramente protegida de ponta a ponta e não ter qualquer impacto no encaminhamento, uma vez que a fronteira criptográfica está fora da rede tática e é transparente para o canal de comunicação. Uma das principais desvantagens é que a gestão de chaves é mais complexa do que no caso em que um único dispositivo criptográfico protege vários anfitriões, porque cada anfitrião precisa de uma chave diferente e válida para cada associação de segurança. Outra desvantagem é o facto de ser muito dispendioso avaliar, certificar e ter a segurança acreditada para um grande número de hospedeiros finais [3].



Proteção ao nível de rede: A proteção ao nível da rede consiste na abordagem IPsec tradicional e baseia-se em encriptadores da camada de rede que separam a rede num lado vermelho e num lado preto. Todos os dados do lado RED são protegidos de ponta a ponta entre os encriptadores de rede.

Uma vantagem desta solução é que uma única unidade de criptografia pode proteger vários anfitriões e aplicações numa CC (lado RED) e os dados encriptados podem ser transmitidos através de qualquer rede não segura. A gestão das chaves é também mais simples do que no caso anterior, uma vez que a mesma função de criptografia é utilizada para proteger vários anfitriões. Algumas desvantagens são o facto de esta solução introduzir mais domínios de encaminhamento, nos lados RED e BLACK. E o controlo da rede e a informação de encaminhamento não podem passar livremente entre o lado RED e o lado BLACK sem comprometer a segurança [3].

Proteção ao nível da ligação: A proteção ao nível da ligação incorpora uma estrutura de segurança simples que protege tanto a carga útil do utilizador como os dados vitais de gestão e controlo da rede. Além disso, normalmente impõe uma sobrecarga mínima, o que a torna uma opção mais eficiente em termos de largura de banda do que os métodos de proteção ao nível da rede. Nomeadamente, não coloca desafios de encaminhamento, uma vez que a fronteira criptográfica reside numa camada inferior da pilha de protocolos.

Algumas limitações prendem-se com o facto de fornecer proteção numa base "hop-by-hop" e necessitar de descriptação e recriptação em cada "hop". Consequentemente, assume implicitamente que todo o tráfego pertence ao mesmo domínio de segurança [3].

Topologias propostas e análise

O conteúdo deste capítulo foi recolhido numa visita ao exercício anual ORION23. Através da recolha de requisitos operacionais no terreno, foi possível compreender até que ponto as informações sensíveis são tratadas pelo pessoal militar ao mais baixo nível da hierarquia. Os cenários diferem em complexidade e nível de segurança.

Cenário 1 - Segregação total

Uma vez que os Comandantes de Batalhão e de Brigada já têm acesso ao domínio de classificação de Missão Secreta, nesta solução concentramo-nos na criação de clusters criptográficos para as unidades inferiores numa bolha criptográfica para cada uma delas, como mostra a Figura 2.

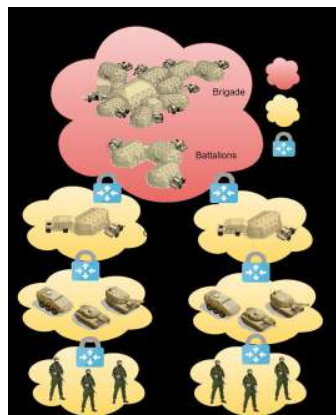


Figura 2 - Topologia de Segregação Completa



Este cenário é adequado para proteger informações sensíveis perto das linhas inimigas. Cada secção forma uma bolha criptográfica utilizando um IEG para proteger a rede se um nó da secção for comprometido.

A comunicação dentro de uma unidade é encriptada para uma missão segura. A comunicação inter-hierárquica passa através de um IEG, permitindo que a unidade de nível superior gira o tráfego de nós comprometidos.

A gestão de chaves é fundamental. A distribuição manual de chaves é uma opção, mas a distribuição automática através de um canal seguro é mais eficiente.

Esta topologia oferece a maior segurança, mas a sua implementação é complexa e dispendiosa. Proporciona um controlo hierárquico para a prevenção de danos, mas exige uma gestão de chaves complexa devido à existência de muitos nós.

Cenário 2 - Segregação completa simplificada

Nesta abordagem alternativa, a configuração difere significativamente da anterior, tornando-se distinta devido ao reduzido número de nós que requerem chaves criptográficas e proteção. Deixando a comunicação entre os pelotões e secções com métodos menos seguros já utilizados (Figura 3).

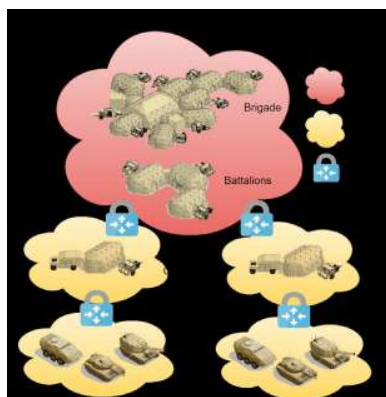


Figura 3 - Topologia de segregação completa simplificada

Este cenário é adequado para os pelotões que tratam de informações sensíveis. As informações das secções são consideradas menos críticas. Dentro da mesma unidade, os dados são encriptados. A comunicação inter-hierárquica passa através de um IEG, permitindo que o superior unidade de nível para gerir o tráfego de nós comprometidos.

A criação de chaves pode ser manual, reduzindo significativamente o número de chaves a distribuir. Isto simplifica a gestão de chaves. Esta configuração simplificada oferece uma segurança robusta com controlo hierárquico. Em caso de compromisso, a unidade de nível superior pode desligar rapidamente a unidade comprometida.



Cenário 3 - Segregação de companhias

Nesta solução alternativa, as Brigadas e dos Batalhões continuam com acesso à classificação de *Mission Secret*, enquanto se criam bolhas criptográficas individuais para cada Companhia comunicar em segurança com as respectivas subunidades, operando dentro de um domínio de classificação de *Mission Restricted*. Esta abordagem assegura que a informação sensível permanece bem protegida e isolada do acesso não autorizado, Figura 4.

Esta solução é o caso de utilização mais simples e mais provável, uma vez que os pelotões e as companhias são altamente móveis e o seu tráfego não requer um IEG.

Ao contrário de outros cenários, este apenas necessita de um IEG entre os batalhões e as suas companhias. A largura de banda limitada disponível para as unidades inferiores acrescenta um constrangimento mínimo devido aos dispositivos de encriptação. Esta solução simplifica a gestão de chaves e é económica para a aquisição de produtos, à semelhança do segundo cenário.

Estas topologias são ideais para unidades envolvidas em missões de Inteligência, Vigilância, Aquisição de Alvos e Reconhecimento (ISTAR), Sistemas de Artilharia e Forças Especiais. Asseguram a comunicação segura para dados altamente classificados, a integridade dos dados para a definição de alvos de precisão e a confidencialidade para operações nas profundezas do território inimigo. Estes cenários têm como objetivo alargar as comunicações seguras às tropas que manuseiam informações sensíveis.

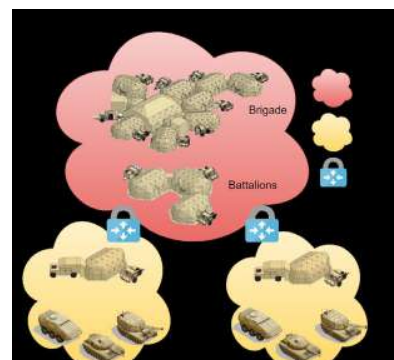


Figura 4 - Topologia de segregação das companhias

Emulação e avaliação de topologias

Este capítulo centra-se na compreensão das limitações de desempenho das redes militares táticas quando a encriptação é introduzida entre os nós. O software utilizado é o *Common Open Research Emulator* (CORE), desenvolvido pela U.S. Naval Research Laboratory baseado em Linux. Foi criada uma topologia de rede semelhante a uma rede tática de batalhão, incorporando nós do Sistemas de Informação de Comunicação Táticos (SIC-T).

As condições de rede são simuladas com uma WLAN de 2 Mbps simulando a utilização de rádios de banda larga. São analisados os tráfegos TCP e UDP. A avaliação dos parâmetros da rede teve como objetivo testar o “stress” da rede, ajustando definições como a perda de pacotes, o atraso e o tráfego simultâneo entre nós.

Atraso nodal: Em termos de atraso nodal, foram consideradas quatro fontes: atraso de processamento, atraso de fila, atraso de transmissão e atraso de propagação. O atraso nodal do tráfego TCP apresentou uma relação inversa com a largura de banda disponível. Atrasos menores tiveram um impacto significativo na largura de banda, afetando particularmente as aplicações em tempo real. O aumento do atraso diminuiu a adequação do TCP para aplicações em tempo real, enquanto o tráfego UDP demonstrou resiliência ao atraso, tornando-o adequado para aplicações em tempo real, apesar da potencial perda de pacotes e do *jitter*. Resultados na Figura 5.

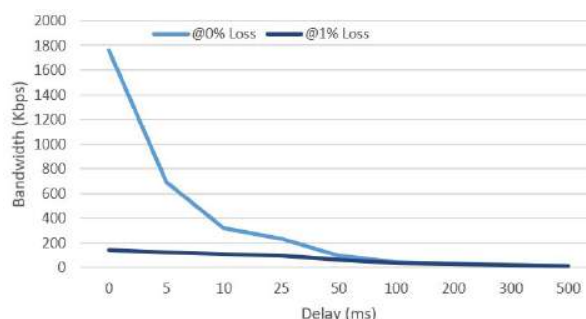


Figura 5 - Impacto do atraso nodal na largura de banda



Perda de pacotes: Relativamente à perda de pacotes, o estudo aumentou sistematicamente a probabilidade de perda de ligações para investigar o seu impacto. Verificou-se que as redes táticas são muito sensíveis às perdas de ligações, o que resulta numa redução da largura de banda para os protocolos TCP e UDP. O desempenho do TCP degradou-se mais rapidamente com o aumento da perda de ligação, enquanto o UDP sacrificou a integridade dos dados, mas lidou ligeiramente melhor com a perda de ligação.

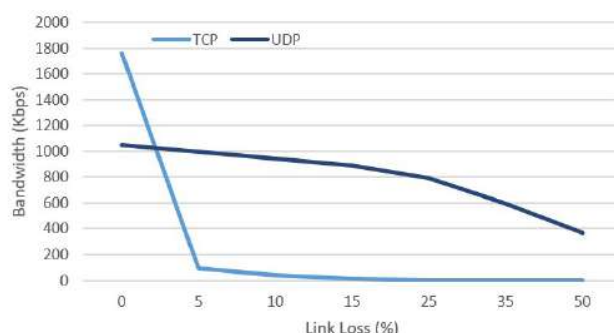


Figura 6 - Impacto da perda de pacotes na largura de banda

Congestionamento da rede: O estudo também explorou o congestionamento da rede, examinando o impacto da comunicação de vários utilizadores com um único Centro de Comunicações de Companhia (CCC). A largura de banda por utilizador diminuiu à medida que mais utilizadores se juntaram, indicando congestionamento. Ocorreu uma queda significativa da largura de banda quando se passou de 3 para 4 utilizadores. A atribuição de maior largura de banda por utilizador melhorou a experiência individual, mas tornou-se ineficiente com mais utilizadores. A atribuição de menos largura de banda por utilizador suporta mais utilizadores, mas pode reduzir o desempenho geral. O tráfego utilizado por cada utilizador na emulação consistiu numa distribuição de Poisson centrada nas larguras de banda especificadas na figura 7.

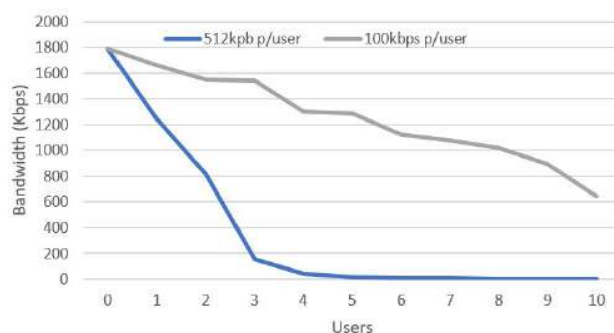


Figura 7 - Impacto do aumento de utilizadores na largura de



Encriptação na rede tática

Este estudo não emulou o tráfego de rede encriptado, mas podem ser tiradas algumas conclusões a partir das características da rede. Partindo do princípio de que a encriptação aumenta o tamanho dos pacotes de dados em cerca de 10-20%, o que leva a uma redução proporcional da largura de banda. Por exemplo, um utilizador com 512 kbps poderá ter cerca de 435 kbps após a encriptação ($512 \text{ kbps} * 0,85$). Da mesma forma, um utilizador com 100 kbps, o utilizador teria cerca de 85 kbps após a encriptação.

Partindo do princípio de que a encriptação acrescenta um atraso de processamento tanto no emissor como no recetor, normalmente de 5-15 ms, aumentando potencialmente a latência da rede de 25 ms para 30-40 ms.

O hardware moderno com aceleradores criptográficos pode reduzir o impacto da latência. A encriptação mais forte aumenta a sobrecarga, mas oferece melhor segurança. Certos protocolos de encriptação podem introduzir atrasos durante o estabelecimento da sessão devido à troca de chaves.

Em conclusão, a encriptação pode afetar a largura de banda e a latência, mas o hardware e a configuração adequados podem atenuar estes efeitos. É essencial efetuar testes minuciosos para garantir que a experiência do utilizador não é afetada, dada a sensibilidade da rede às restrições de latência e largura de banda.

Conclusão

Este estudo teve como objetivo explorar o alargamento dos domínios classificados às unidades militares inferiores, afirmando a sua viabilidade.

O estudo incluiu três fases: revisão da literatura, trabalho de campo e emulação de rede tática. Os resultados mostram que a integração da encriptação ligeira é viável, tendo em conta as limitações de largura de banda.

A investigação futura pode centrar-se na aplicação em cenário real de máquinas de cifra de modo a obter resultados experimentais reais.

O estudo concluiu que a encriptação deve ser muito leve devido à baixa largura de banda, latência e sobrecarga desta tipologia de redes (com protocolos de cifra que ocupem no máximo 20% dos pacotes e que não introduzam latências superiores a 40ms).

Referências

[1] Arjen Holtzer, Ronald In't Velt, Floris Drijver, Henning Rogge, Jonathan Kirchhoff, Christoph Barz, Niels Van Adrichem, and Mariann Hauge. *Tactical router interoperability: Concepts and experiments*. In *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, pages 647–654, 2018.

[2] Roland Schutz, Sam McLaughlin, Tim Daeleman, Marko Luoma, Markus Peuhkuri, Per Carlen, and John Haines. *Protected core network- ing (pcn): Pcn qos and sla definition*. In *2013 Military Communications and Information Systems Conference*, pages 1–9, 2013.

[3] Anne Marie Hegland, Mariann Hauge, and Arjen Holtzer. *Federating tactical edge networks: Ways to improve connectivity, security, and network efficiency in tactical heterogeneous networks*. *IEEE Communications Magazine*, 58(2):72–78, 2020.

EyeCommand

Suite de Comando e Controlo (C4I) que proporciona às forças de defesa um conhecimento situacional otimizado em todos os níveis da cadeia de comando. Oferece, também, um quadro operacional comum, facilitando a tomada de decisões mais rápidas e eficazes, a nível tático e a nível operacional.



Melhora a perceção do panorama situacional

Integra com o Soldier System

Melhora a interoperabilidade

Adapta-se às necessidades do Exército Português

Permite interoperabilidade com sistemas NATO

Uma solução tática para forças terrestres, simples de utilizar, ideal para dispositivos leves e ecrãs pequenos, que dá apoio a elementos operacionais desmontados.

www.criticalsoftware.com



Critical
software



Técnicas de Calibração para um Novo Radar Espacial com Sistema de Direcionamento para Antena Cassegrain

Alferes-Aluno Tm Nilton Bárbara
TPO Transmissões

Resumo - Este artigo investiga a adequação do sistema de radar localizado na Pampilhosa da Serra para integração em Sistemas de Defesa contra Mísseis Balísticos (BMDS). No centro deste estudo está uma simulação desenvolvida em MATLAB, concebida para replicar a trajetória do míssil e os desafios no seu rastreio usando sistemas de radar. Através de uma série de cenários simulados, o estudo explorou o desempenho do Filtro de Kalman Estendido (EKF) no rastreio de mísseis. As principais métricas de desempenho, incluindo o erro quadrático médio (RMSE), o erro absoluto médio (MAE) e o erro de estimativa normalizado ao quadrado (NEES), foram utilizadas para avaliar a precisão do rastreamento. Em particular, nas configurações de radar selecionadas, os valores de RMSE baixaram para 41 metros, o MAE foi reduzido para 37 metros e o NEES melhorou significativamente para cerca de 1.5. Estas métricas sublinham o impacto das características do radar na precisão do rastreamento e sugerem a potencial eficácia do sistema de radar da Pampilhosa da Serra em aplicações BMDS quando devidamente configurado.

I. Introdução

Radio Detection and Ranging, mais vulgarmente conhecido como Radar, é a palavra utilizada para descrever sistemas que fazem uso da transmissão de ondas eletromagnéticas dirigidas a uma área de interesse. Um radar padrão faz uso de um transmissor, uma antena, um recetor e um processador de sinal. O objetivo de um radar é fazer com que a onda produzida pela sua antena atinja um potencial objeto de interesse, provocando a dispersão da onda e depois de receber parte da onda dispersa, aplicar diferentes ferramentas para o processamento de sinal e tratamento de dados, com o intuito de detetar, localizar, seguir e reconhecer vários objetos.

A. Objetivo

Este trabalho centra-se no aspeto crucial da defesa contra mísseis balísticos, especificamente, nas técnicas de calibração utilizadas para os sistemas de direcionamento das antenas, neste caso *cassegrain*, dos radares. O objetivo é aprofundar a compreensão dos atuais métodos e identificar áreas que possam ser melhoradas. Este trabalho avaliará as limitações e os desafios associados a estas técnicas e terá também como objetivo desenvolver um novo método de calibração que aborde estas questões e proporcione maior exatidão e precisão. A eficácia do método será testada através de simulações e serão feitas recomendações práticas para a sua implementação em futuros sistemas de radar.



II. Antecedentes

Na sua essência, o mecanismo fundamental do funcionamento de um radar reside na emissão destas ondas e na análise subsequente dos sinais refletidos ou "ecos" que regressam dos objetos visados, que interrompem e dispersam a frente de onda. Quando uma onda eletromagnética emitida encontra um objeto, parte da energia da onda é desviada de volta para o radar, transportando consigo informação sobre as propriedades do objeto. O tempo necessário para que a onda emitida viaje até ao objeto e depois regresse como onda refletida fornece uma medida direta da distância ou do alcance desse objeto. Além disso, utilizando o efeito *Doppler* (uma mudança de frequência para objetos em movimento), a velocidade radial de um alvo pode ser determinada, oferecendo informações sobre o seu movimento.

A. Antena Cassegrain:

Utiliza um refletor secundário convexo (sub-refletor) colocado entre o refletor parabólico principal e a alimentação, tal como pode ser visto na Figura 1.

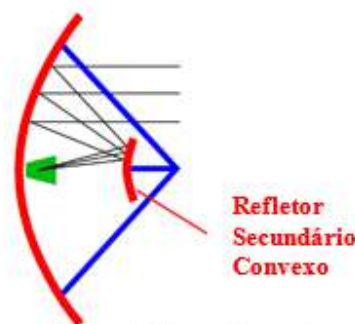


Figura 1: Antena Cassegrain

B. Mísseis balísticos

Um míssil balístico é um projétil que segue uma trajetória suborbital, trajetória essa que pode ser dividida em três fases principais. A fase de *boost*, durante a qual o míssil atinge a sua velocidade máxima sendo apenas alimentado pelo seu sistema de propulsão. A fase intermédia, durante a qual o míssil deixa de ser alimentado e segue uma trajetória balística sob a influência da gravidade, podendo durar desde alguns minutos até horas. A fase terminal, no final desta fase, a carga do míssil atinge o alvo, com um impacto a uma velocidade de até 7 km/s.

III. Metodologia

A metodologia proposta implicou o desenvolvimento de um ambiente de simulação simples, expandindo-o até chegar a uma simulação mais avançada que representa um cenário real o mais próximo possível. Depois de concluída a simulação, seguiu-se a implementação de um radar e subseqüentes medições do mesmo. O algoritmo do Filtro de Kalman Estendido foi implementado na simulação com base nas medições do radar e, a partir da trajetória estimada, foram analisadas várias estatísticas.



A fim de focar na parte mais importante do objetivo principal deste artigo, foram estabelecidos alguns pressupostos:

Em primeiro lugar, a simulação inicia a análise da trajetória do míssil após a fase de *boost*, uma decisão que tem por base tanto a simplificação do modelo computacional como a relevância para o mundo real. A omissão da fase de *boost* ajuda a evitar a complexidade da modelação da aceleração rápida e da dinâmica de transição atmosférica presentes desde o lançamento, fornecendo uma estrutura computacionalmente mais tratável e mantendo elementos essenciais do voo do míssil.

Em segundo lugar, o sistema de radar foi hipoteticamente posicionado perto do ponto de impacto do míssil previsto, uma suposição baseada no planeamento estratégico de defesa, onde os radares são frequentemente colocados para salvaguardar infraestruturas críticas ou áreas densamente povoadas. Neste cenário, o posicionamento dos radares é crucial para otimizar as probabilidades de deteção e melhorar as medidas defensivas preventivas.

IV. Resultados

De forma a melhor estudar a implementação do EKF e se este é um algoritmo válido para ser utilizado no tracking de mísseis balísticos, foram efetuadas várias simulações, dividindo-as em 7 casos de estudo, cada um com um parâmetro específico a estudar. Em todos os casos, alguns valores mantiveram-se constantes. As simulações foram efetuadas com 30 parâmetros constantes, alguns dos quais podem ser vistos na Tabela 1.

TABELA 1: VALORES CONSTANTES DA SIMULAÇÃO

v_0	7000 m/s
ϕ	300 deg
θ	45 deg
Lat	40.105784 deg
Lon	127.066978 deg
x_{radar}	$7.5554 \times 10^6 m$
y_{radar}	$8.1046 \times 10^6 m$
z_{radar}	0 m
L	1.3
$Range_{\text{max}}$	$1000 \times 10^3 m$
C_d	0.15
m	362 kg
x	4274030.934 m
y	14512235.624 m
z	170000 m

Onde v_0 é a velocidade de lançamento, ϕ o ângulo de azimuth do lançamento, θ o ângulo de elevação do lançamento, Lat é a latitude da posição de lançamento, Lon é a longitude da posição de lançamento, x_{radar} , y_{radar} e z_{radar} a posição do radar, L o fator de perda do radar, $Range_{\text{max}}$ o alcance máximo do radar, C_d o coeficiente de drag do míssil, m a massa do míssil e x, y e z a posição inicial do míssil após a fase de boost.



A Figura 2 mostra a trajetória do míssil simulado que foi estudado e ao qual foi aplicado o EKF. Depois de simular a trajetória e o comportamento do míssil balístico, é possível obter alguns dados tal como constam na Tabela 2.

Figura 2: Trajetória do míssil

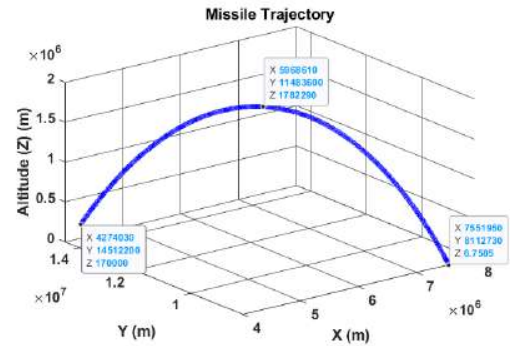


TABELA 2: ESTATÍSTICAS DA TRAJETÓRIA DO MÍSSIL

Tempo total de voo	Distância percorrida no solo	$Speed_{Max}$	$height_{Max}$	Ponto de impacto
1497.1 s	11.0837×10^6 m	7137,94 m/s	17.82×10^5 m	$[7.5, 8.1, 0] \times 10^6$ m

Os sete casos diferentes simulados variam todos em algum aspeto, com o objetivo de estudar o impacto que um radar com parâmetros diferentes tem no desempenho do EKF. Os parâmetros estudados nos sete casos são o alcance mínimo de deteção, Range_min a potência transmitida no pico, P_peak e a Secção Transversal do Radar (RCS) do míssil, σ .

A. Casos estudados

Para o Caso A, o objetivo principal foi simular as condições que estão presentes no sistema de radiotelescópio do observatório astronómico da Pampilhosa da Serra para ver se a estação pode servir como um radar apropriado para ser usado num sistema de defesa de mísseis balísticos e, ao mesmo tempo, atuar como um caso de controlo. Os casos B, C e D servem para ver o efeito que o RCS (σ) do míssil pode ter no desempenho do algoritmo. O objetivo principal do caso E era observar o efeito que o alcance mínimo de deteção do radar tinha no desempenho do EKF. O caso F tinha como objetivo principal observar o efeito que a potência de pico do radar tinha no desempenho do EKF. O caso G, o último caso, tinha como objetivo observar o comportamento do filtro no melhor cenário possível, com um valor inferior para o alcance mínimo de deteção e um valor superior para a potência de pico do radar.

A Tabela 3 apresenta as variáveis para os sete casos.

TABELA 3: VARIÁVEIS DA SIMULAÇÃO

Casos	$Range_{min}$	P_{Peak}	σ
A	50×10^3	5×10^3	10
B	50×10^3	5×10^3	1
C	50×10^3	5×10^3	100
D	50×10^3	5×10^3	1000
E	50×10^{-3}	5×10^3	10
F	50×10^3	5×10^6	10
G	50×10^{-3}	5×10^6	10



B. RMSE vs. tempo

O RMSE fornece uma medida quantificável que indica até que ponto as previsões do EKF se aproximam da verdadeira trajetória do míssil, o que o torna uma ferramenta valiosa para avaliar a robustez do sistema de rastreamento. Na Figura 3 é possível ver como o valor de RMSE varia no caso G. Na Tabela 4, é possível ver como os valores de RMSE variam nos 7 casos.

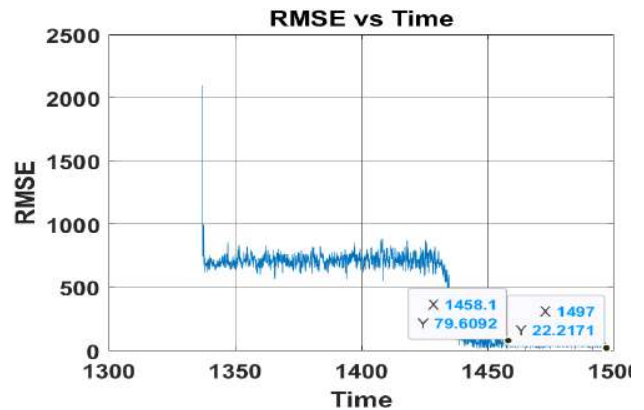


Figura 3: Valores RMSE em função do tempo

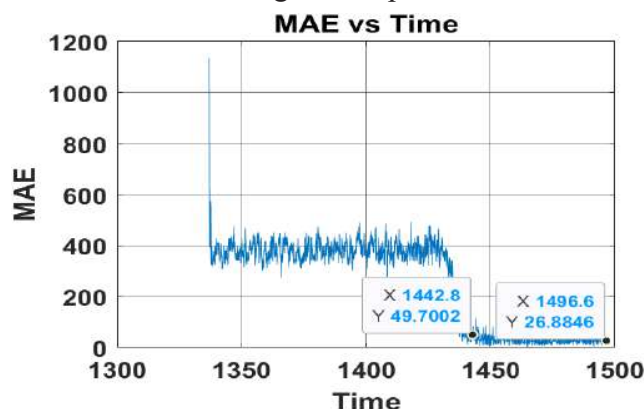
TABELA 4: VALORES GLOBAIS DE RMSE

Casos	OverallRMSE(m)	Trackingwindow(s)
A	732.2431	10.5
B	831.4352	3.5
C	798.1098	24.2
D	736.3096	48.9
E	320.2124	75.6
F	724.3738	94.4
G	563.8943	160

Os valores mais elevados de RMSE dos casos com pior desempenho, A, B, C, D e F, resultam do facto de a distância mínima de deteção de 50 km não ser suficientemente baixa para captar a redução de velocidade que o míssil sofre devido à força de drag que atua nele ao reentrar na atmosfera. Para o caso G, há uma queda notável no RMSE em torno da marca de 1435 s. Após esta queda, forma-se um novo patamar inferior onde o RMSE estabiliza novamente, passando de uma média de 750 m para uma média de 35 m. Embora os valores absolutos de RMSE possam diferir de um caso para outro, o comportamento geral nas simulações permanece consistente.

C. MAE vs. tempo

O MAE oferece uma medida simples que quantifica a magnitude média dos erros entre as previsões da EKF e a trajetória real do míssil. Na Figura 4 é possível ver como o valor de MAE



varia no caso G. Na Tabela 5, é possível observar como os valores do MAE variam nos 7 casos.

TABELA 5: VALORES MAE GLOBAIS

Casos	Overall MAE(m)
A	384.4747
B	415.2629
C	396.4206
D	385.6785
E	98.5622
F	381.4597
G	248.5942

Figura 4: Valores MAE em função do tempo



Os valores mais elevados de MAE nos casos A, B, C, D e F podem ser atribuídos à reentrada atmosférica do míssil em 1435 s não ter sido observada. No entanto, os casos E e G, que têm uma distância de detecção menor, mostram uma redução notável nos valores de MAE.

O caso E, que capta a reentrada atmosférica do míssil, apresenta o MAE médio mais baixo de 98.5622 m.

D. NEES vs. tempo

O NEES fornece uma medida normalizada para avaliar a exatidão das estimativas de estado em comparação com a sua exatidão esperada. Essencialmente, ele quantifica o quanto a incerteza interna do EKF (covariância) corresponde aos erros de estimativa reais. Ao utilizar o EKF para o *tracking* da trajetória de mísseis, é crucial não só ter estimativas precisas, mas também que o filtro seja consciente da sua própria precisão. Um filtro bem calibrado terá valores NEES próximos da dimensão da matriz de incerteza, indicando que o erro de estimativa é consistente com a incerteza. Na Figura 5 é possível ver como o valor de NEES varia no caso G.

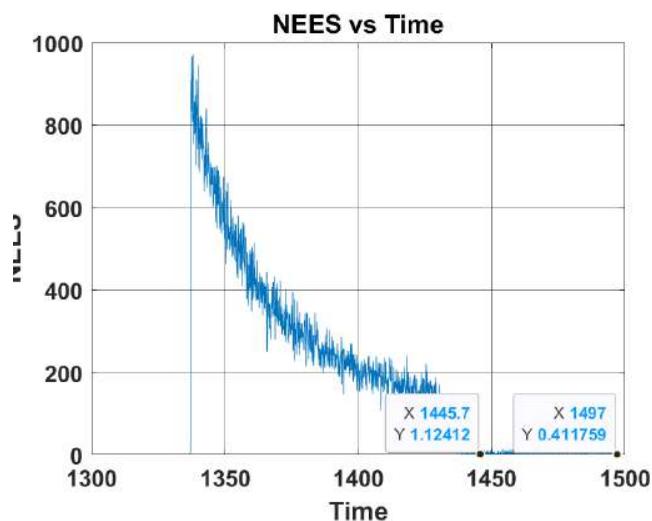


Figura 5: Valores NEES em função do tempo

A análise do gráfico NEES revela padrões que são distintos dos gráficos RMSE e MAE observados anteriormente. Em vez de observar um pico, os valores NEES começam relativamente baixos.

O gráfico pode ser dividido em duas fases principais. A primeira fase, que vai até aos 1435 s observa um decréscimo exponencial dos valores. Este decréscimo, embora consistente, torna-se menos pronunciado com o tempo, reduzindo gradualmente a taxa de diminuição do NEES. É importante notar que este comportamento é exclusivo dos gráficos NEES e não foi observado nos gráficos RMSE e MAE.

Ao atingir 1435 s os casos E e G, os únicos que ultrapassam este ponto, apresentam uma queda acentuada nos valores NEES. Após esta queda, estes casos entram num patamar estável com valores que variam entre 0.4 e 22. Este patamar indica um período de relativa estabilidade e flutuação mínima nos erros de previsão do Filtro de Kalman Estendido. Para os casos que não vão além de 1435 s os valores do NEES permanecem consideravelmente elevados.



V. Conclusões

Enquanto o Caso A forneceu uma linha de base, os casos subsequentes (B a G) introduziram variações nas especificações do radar, simulando potenciais melhorias que poderiam ser efetuadas.

As métricas iniciais do Caso A não eram as ideais. Com um RMSE de 700 metros, MAE de 369 metros, e um NEES de 5.13695×10^5 a necessidade de melhoria era evidente.

Um RMSE de 700 metros implica que, em média, as previsões do radar têm uma magnitude de erro típica de 700 metros. Num cenário BMDS, este é um erro substancial. Quando se lida com mísseis em movimento rápido, um erro de avaliação de 700 metros pode fazer a diferença entre uma interceção bem sucedida e uma falha.

Um MAE de 369 metros indica que o sistema de radar, em média, erra a posição real do míssil em 369 metros. Esta margem de erro pode ser crítica quando o objetivo é intercepar o míssil com precisão.

Um NEES de 5.13695×10^5 é extremamente elevado. Esse valor sugere que os erros de estimativa do EKF são muito maiores do que o que o filtro prevê, indicando que o estimador está muito pouco confiante.

Para um BMDS, esta é uma preocupação grave. Um valor elevado de NEES não só aponta para imprecisões no rastreamento, como também destaca um problema fundamental com a capacidade do sistema para compreender e quantificar as suas próprias incertezas. Se um sistema de defesa não consegue prever com fiabilidade a trajetória de um míssil ou compreender a magnitude dos seus próprios erros de previsão, isso pode conduzir a vulnerabilidades significativas, como interceções mal sucedidas ou, pior ainda, falsa confiança numa interceção bem sucedida quando esta não ocorreu.

No entanto, à medida que as especificações do radar foram ajustadas nos casos subsequentes, registaram-se grandes melhorias. Em particular, no caso G que apresenta melhorias significativas, com os seus valores RMSE a descenderem para apenas 41 metros e os seus valores NEES a aproximarem-se do valor ótimo de 1 e, por vezes, a permanecerem abaixo dele.

No contexto dos padrões da indústria, comparando com simulações efetuadas para um radar com especificações como as dos Gap Filling Tracking Radars (GFTR), um valor de RMSE inferior a 50 metros é considerado desejável. Os resultados deste artigo, particularmente no caso G, atingiram este valor de referência, indicando as potencialidades do sistema de radar da Pampilhosa da Serra quando complementado com as especificações corretas. Comparando as especificações do sistema de radar da Pampilhosa da Serra, representado no caso A, com as especificações dos *Gap Filling Tracking Radars* (GFTR) [6] obtém-se a seguinte Tabela 6.

TABELA 6: COMPARAÇÃO GFTR

Especificações	Pampilhosa	GFTR-2100/48	GFTR-2100/51	GFTR-2100/54
<i>Range(km)</i>	1000	1400	2200	4000
<i>Accuracy_{range}(m)</i>	75	<0.5	<0.5	<0.5
<i>Accuracy_{angle}(rad)</i>	0.1	<0.0001	<0.0001	<0.0001
<i>Accuracy_{velocity}(m/s)</i>	1000	<0.1	<0.1	<0.1
<i>Range_{resolution}(m)</i>	1000	1	1	1
<i>Velocity_{resolution}(m/s)</i>	1000	1	1	1
<i>Beamwidth(deg)</i>	0.73	0.67	0.5	0.33



V. Referências bibliográficas

- [1] R. L. McCoy, *Modern exterior ballistics: The Launch and Flight Dynamics of Symmetric Projectiles*. Schiffer Military History, 2012.
- [2] G. Joos and I. M. Freeman, *Theoretical Physics*. Courier Corporation, 1986.
- [3] W. Menke and D. Abbott, *Geophysical theory*. 1990.
- [4] B. F. Edwards and J. Edwards, "Forces and conservation laws for motion on our spheroidal Earth," *American Journal of Physics*, vol. 89, no. 9, pp. 830–842, Sep. 2021, doi: 10.1119/10.0004801.
- [5] C. K. Chui and G. Chen, *Kalman filtering: with Real-Time Applications*. Springer, 2017.
- [6] "Ground-based Ballistic Missile Defense - Long-range radar," Weibel - Doppler Radars. <https://weibelradars.com/explore-ballistic-missile-defense/ground/ground/> (accessed Oct. 31, 2023).





Cluster de características de eventos do Windows e NetFlow definidos dinamicamente para detecção de intrusões

Alferes-Aluno Tm João Pinheiro
TPO Transmissões

Resumo-Nos últimos anos, tem havido um notável aumento nos ciberataques em todo o mundo, tornando as organizações mais suscetíveis a ameaças virtuais em constante evolução. A proteção das redes contra tais ataques é crucial, e os Sistemas de Detecção de Intrusões (SDIs) desempenham um papel vital nesse cenário dinâmico. Este estudo visa destacar as vantagens da integração dos Eventos do *Microsoft Windows* (EMSWs) nos atuais SDIs, aproveitando a riqueza de dados disponíveis. Os EMSWs oferecem uma visão aprofundada do comportamento das máquinas Windows da Microsoft, enquanto o sistema proposto realiza a extração dinâmica de características tanto do anfitrião quanto da rede. Comparado a abordagens semelhantes de alto desempenho, o sistema proposto demonstra um aumento de 3% na pontuação F1, 5% na recuperação e uma precisão equivalente. Estes resultados destacam as contribuições significativas deste trabalho para o campo dos SDIs.

Palavras-chave- Cibersegurança, Aprendizagem automática, Sistema de detecção de intrusões, Análise de segurança, Netflow, Registos.

I. Introdução

Com a crescente dependência da tecnologia, surge a necessidade de melhores sistemas de segurança. A inevitável digitalização dos processos de cada organização expõe-nas a ciberataques que podem comprometer o funcionamento e a segurança dessa organização.

Os sistemas tradicionais de detecção de intrusões (SDIs) utilizam características dos dados da rede ou características recolhidas dos anfitriões para detetar possíveis ataques à rede. O presente trabalho tem como objetivo fundir dados de rede e dados do anfitrião para aplicar técnicas de aprendizagem automática a fim de produzir uma nova e melhorada abordagem de detecção de intrusões para detetar ataques invisíveis, proporcionando um sistema fiável, preciso e eficiente.

II. Antecedentes

Esta secção descreve conceitos básicos fundamentais para compreender o desenvolvimento e a aplicação da abordagem proposta.

A. Fluxos de rede

Os fluxos de rede são uma fonte de dados popular para os sistemas de detecção de intrusão de rede (SDIR). A exportação de fluxos é uma abordagem passiva de monitorização da rede em que os pacotes são agrupados em fluxos e exportados para armazenamento e análise [1].

B. Eventos do Microsoft Windows

O Microsoft (MS) Windows é o sistema operativo mais popular para computadores fixos e portáteis em todo o mundo e, como tal, é visado com mais frequência pelos autores de malware do que outros sistemas operativos [2]. Por conseguinte, a incorporação dos eventos do *Microsoft Windows Log* (EMSWL) no SDI proposto é do maior interesse.



C. Sistemas de detecção de intrusão

Soniya define SDI como "uma arte de detetar as atividades dos intrusos" [3]. Um SDI é o processo de monitorização de eventos ocorridos numa rede ou sistema informático para detetar sinais de atividades maliciosas. Existem três SDIs principais [4]:

- SDIR: Os SDIR recebem dados do tráfego de rede e monitorizam o sistema global ou as comunicações de rede com um baixo custo de implementação.
- Os sistemas de detecção de intrusões no anfitrião (SDIA) podem monitorizar o comportamento interno de um computador, detetando ataques internos e outros ataques que podem não ser detetados pelos SDIR tradicionais.
- Os sistemas de detecção de intrusões baseados em clusters são sistemas que aplicam algoritmos de cluster nas características extraídas da população de uma rede para detetar e assinalar anomalias.

D. Aprendizagem automática

As técnicas de aprendizagem automática são utilizadas principalmente na abordagem proposta para agrupar as máquinas que pertencem à rede. O cluster é um processo em que os objetos com um comportamento semelhante são agrupados com base em características pré-selecionadas. Após o cluster, as ocorrências que não pertencem a nenhum cluster são classificadas como anomalias.

III. Solução proposta

Esta secção descreve a solução proposta. Inclui uma descrição geral e uma descrição pormenorizada da arquitetura proposta e uma descrição da implementação da abordagem proposta.

A. Descrição geral

Os fluxos de rede são uma fonte de dados popular para os sistemas de detecção de intrusão de rede (SDIR). A exportação de fluxos é uma abordagem passiva de monitorização da rede em que os pacotes são agrupados em fluxos e exportados para armazenamento e análise [1].

A abordagem proposta difere das publicações analisadas ao integrar dados do anfitrião e da rede num sistema único com características de rede e anfitrião selecionadas dinamicamente. A Figura 1 apresenta a arquitetura proposta:

1. Primeiro, a extração dinâmica das características baseadas na rede e no anfitrião, que são adicionadas a um conjunto de características fixas.
2. Em seguida, o cluster é aplicado aos vetores de características, em que cada vetor representa uma máquina ou um utilizador. Depois disso, são implementados os três algoritmos de cluster.
3. Em seguida, os vetores que satisfazem os critérios de outlier, descritos a seguir, são assinalados como ocorrências positivas.

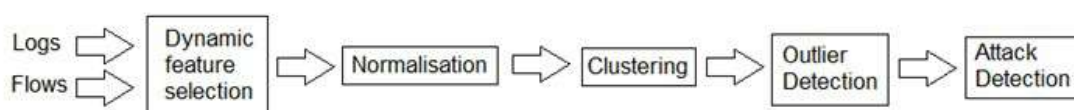


Figura 1. Descrição geral da proposta.



B. Descrição pormenorizada

Esta secção apresenta uma descrição mais pormenorizada da abordagem proposta (Figura 1).

1) Seleção dinâmica de características

O sistema proposto define dinamicamente as características do anfitrião e da rede. Enquanto no DYNIDS [5], apenas foram utilizadas características da rede, no sistema proposto é estabelecido um procedimento para integrar a seleção de características do anfitrião.

Para as características da rede, são extraídas 12 características fixas e um número variável de características dinâmicas. Quatro características são definidas dinamicamente para cada porta selecionada em tempo de execução, proporcionalmente ao número de portas. O número ideal de portas selecionadas (x) é 100, como indicado pelo DYNIDS [5].

A seleção de características do anfitrião segue a mesma lógica que a seleção de elementos para os dados da rede. São definidas sete características fixas para os dados do anfitrião. Para além destas características fixas, estão incluídas características definidas dinamicamente. O número total destas características (x) é definido em tempo de compilação (antes do tempo de execução).

2) Cluster

Após a normalização das características, estão reunidas as condições para aplicar o algoritmo de *clustering* e identificar os valores atípicos que podem representar uma atividade maliciosa. O objetivo do *clustering* é agrupar máquinas com comportamento semelhante. O sistema utiliza uma combinação de diferentes algoritmos (*K-Means*, *Agglomerative* e *DBSCAN*).

3) Detecção de *Outlier*

Este trabalho apresenta quatro métodos possíveis para ultrapassar a dificuldade de selecionar o cluster de vítimas. Os métodos propostos são:

1. Método de clusters de um elemento: Os clusters de um elemento serão classificados como anómalos.
2. Pontuações das máquinas: Medição das pontuações das máquinas com base na população do respetivo cluster em cada algoritmo.
3. Método do coeficiente de Silhueta: Medição do coeficiente médio de Silhueta para cada cluster em cada algoritmo.
4. Método de baixa população: Seleção de clusters com menos de dez elementos.



IV. Avaliação experimental

Nesta secção, são calculadas as métricas de avaliação para os resultados obtidos pela abordagem proposta com dados do anfitrião e com a combinação de dados do anfitrião e da rede.

A. Métricas de avaliação

Esta secção apresenta as métricas de avaliação utilizadas para medir o desempenho do sistema. Estas métricas classificam os resultados obtidos e a eficácia da abordagem. O sistema proposto será avaliado relativamente aos seguintes parâmetros:

- Taxa de verdadeiros positivos;
- Taxa de falsos positivos;
- Precisão;
- Exatidão;
- Recuperação;
- Pontuação F1.

B. Avaliação do sistema tendo em conta os dados do anfitrião

Esta subsecção apresenta os resultados obtidos através da clusterização dos dados do anfitrião do conjunto de dados CSE-CIC-SDI2018.

1) Ataque BOT (02-03-18), dados do anfitrião

Existem dois tipos de ataques aos dias seleccionados do conjunto de dados. O primeiro em análise é o ataque BOT. O ataque classificado como BOT pelo conjunto de dados CSE-CIC-SDI2018 refere-se a um ataque de *botnet* executado em 02-03-2018 que comprometeu dez máquinas.

A Tabela 1 apresenta os resultados obtidos pela abordagem proposta para os dados do anfitrião em 02-03-18 com diferentes valores de x .

TABELA 1. RESULTADOS OBTIDOS COM OS DADOS DO ANFITRIÃO PARA DIFERENTES VALORES DE x PARA CADA ALGORITMO EM 02-03-18.

	K-means			DBSCAN			Aglomerativo		
	Aglomerado	Total	Vítimas	Aglomerado	Total	Vítimas	Aglomerado	Total	Vítimas
$x=20$	1	57	5	-1	14	1	0	88	3
	3	26	2	7	135	7	2	27	2
	6	85	3	12	13	2	3	53	5
$x=30$	1	106	3	0	411	10	0	116	3
	3	73	5	-	-	-	2	27	3
	5	26	2	-	-	-	6	62	4
$x=50$	0	74	5	0	411	10	3	116	3
	2	105	3	-	-	-	4	74	5
	7	26	2	-	-	-	5	15	2
$x=80$	1	72	5	0	413	10	7	17	10
	5	106	3	-	-	-	-	-	-
	6	27	2	-	-	-	-	-	-
$x=10$	1	45	7	0	204	10	3	17	10
	7	164	3	-	-	-	-	-	-



1) Detecção de valores atípicos com dados do anfitrião e $x=100$ em 02-03-18 (BOT)

Após o *cluster*, foram aplicados métodos de deteção de valores atípicos. As pontuações das vítimas demonstram que nenhuma vítima tem uma pontuação inferior a 5% da pontuação média (0,045178).

O terceiro método de seleção do cluster da vítima consiste em analisar o coeficiente de Silhueta médio de cada *cluster* para cada algoritmo. A Figura 2 apresenta os coeficientes de silhueta médios para cada *cluster* do algoritmo K-means.

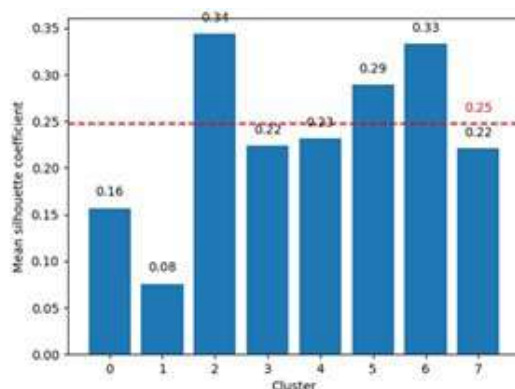


Figura 2. Coeficiente de silhueta médio para os *clusters* no algoritmo K-means para $x=100$ em 02-03-18.

O quarto e último método para a deteção de anomalias considera todos os *clusters* com menos de dez elementos como uma ocorrência positiva. As métricas de avaliação para cada método e para cada algoritmo são apresentadas na Figura 3.

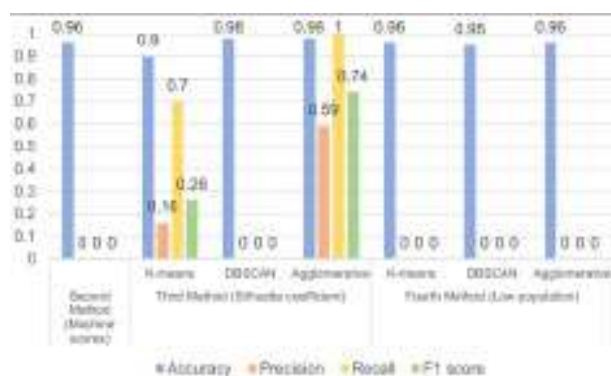


Figura 3. Métricas de avaliação para cada método de deteção de *outlier* no dia 02-03-18 para os dados do anfitrião.

2) Ataque de infiltração (01-03-18), dados do anfitrião

O segundo tipo de ataque é o ataque de infiltração (01-03-18). Num ataque de infiltração, o atacante obtém acesso não autorizado a uma aplicação vulnerável.



3) Resumo dos resultados com dados do anfitrião

Em resumo, os métodos de detecção de anomalias não atingiram o desempenho desejado. O algoritmo Aglomerativo, com o terceiro método, obteve os melhores resultados com uma exatidão de 0,98, uma precisão de 0,59, uma recuperação de 1 e uma pontuação F1 de 0,74. A Figura 4 ilustra os resultados obtidos por cada método em 02-03-18.

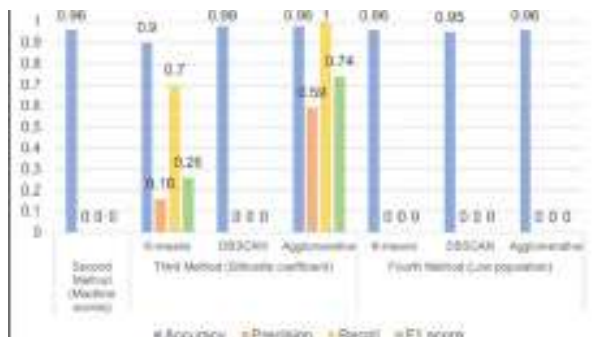


Figura 4. Métricas de avaliação para cada método de detecção de outlier em 02-03-18 para dados do anfitrião.

A Figura 5 compara as métricas de avaliação para todos os métodos de detecção de anomalias em 01-03-18.

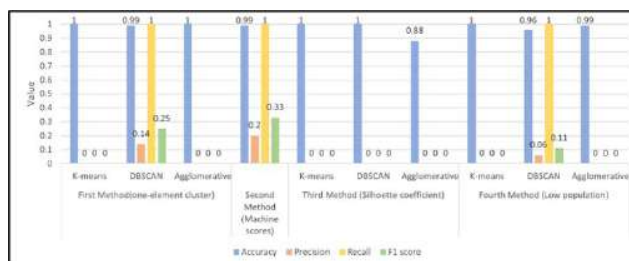


Figura 5. Métricas de avaliação para cada método de detecção de outlier em 01-03-18 para dados do anfitrião.

C. Avaliação do sistema tendo em conta os dados do anfitrião e da rede

Esta secção apresenta os resultados obtidos pela abordagem proposta com dados do anfitrião e da rede.

1) Ataque BOT (02-03-18), dados da rede e do anfitrião

A Tabela 2 ilustra os resultados alcançados pelo cluster das características da rede e do anfitrião para cada algoritmo considerado.

TABELA 2. RESULTADOS DE CLUSTERING PARA O ATAQUE BOT (02-03-18) COM DADOS DE REDE E DE ANFIRIÃO E X=100.

K-means			DBSCAN			Aglomerativo		
Agglomerado	População	Vitima	Agglomerado	População	Vitima	Agglomerado	População	Vitima
0	66	-	-1	3	-	0	159	-
1	22	-	0	204	10	1	38	-
2	39	1	1	203	-	2	38	2
3	39	-	2	4	-	3	32	-
4	73	-	-	-	-	4	61	-
5	135	-	-	-	-	5	6	-
6	7	-	-	-	-	6	23	-
7	9	9	-	-	-	7	8	8
8	32	-	-	-	-	8	41	-
9	1	-	-	-	-	9	7	-



2) Ataque de infiltração (01-03-18), dados da rede e do anfitrião

Neste dia existe apenas uma vítima. Assim, é expetável que um cluster com apenas um elemento criado pelos algoritmos indique uma anomalia. Os resultados obtidos estão ilustrados na Tabela 3.

TABELA 3. RESULTADOS DE CLUSTER PARA OS ATAQUES DE INFILTRAÇÃO (01-03-18) EM DADOS DO ANFITRIÃO E X=100.

K-means			DBSCAN			Aglomerativo		
<i>Aglomerado</i>	<i>População</i>	<i>Vítima</i>	<i>Aglomerado</i>	<i>População</i>	<i>Vítima</i>	<i>Aglomerado</i>	<i>População</i>	<i>Vítima</i>
0	55	-	-1	2	1	0	74	-
1	75	-	0	366	-	1	11	-
2	146	-	1	45	-	2	61	-
3	11	-	-	-	-	3	28	-
4	29	-	-	-	-	4	75	-
5	67	-	-	-	-	5	138	-
6	1	1	-	-	-	6	1	1
7	29	-	-	-	-	7	25	-

3) Resumo dos resultados com dados do anfitrião e da rede

A Figura 6 ilustra os resultados obtidos por cada método de detecção de valores atípicos para os dados do anfitrião e da rede em 02-03-18. O quarto método obteve os melhores resultados. O DBSCAN continua a fornecer resultados fracos no ataque BOT. O elevado número de vítimas parece ter um impacto mais significativo neste algoritmo.

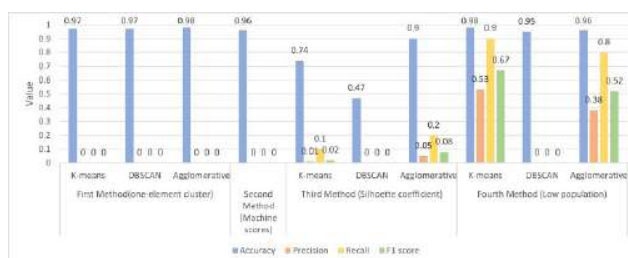


Figura 6. Métricas de avaliação para cada método descrito na subsecção 4.2.4 para dados do anfitrião e da rede em 02-03-18.

O sistema proposto é muito mais eficaz em 01-03-18 (infiltração). Os resultados, apresentados na Figura 7 mostram que o sistema fornece excelentes métricas de avaliação para todos os métodos, exceto para o terceiro. Estes resultados representam uma melhoria em relação a abordagens semelhantes.

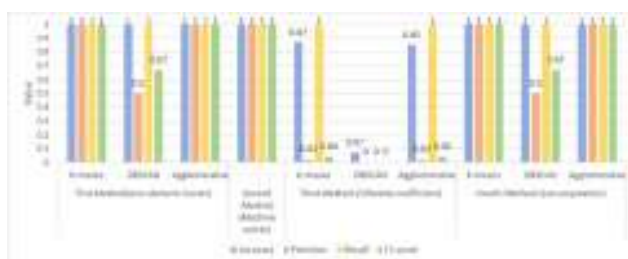


Figura 7. Métricas de avaliação para cada método de detecção de outlier para dados do anfitrião e da rede em 01-03-18.



D. Comparação com diferentes algoritmos

A Figura 8 apresenta as métricas de avaliação alcançadas por vários sistemas para o CSE-CIC-SDI2018. O F1-Score obtido pela abordagem proposta é 3% superior ao F1-Score obtido pelo DYNIDS e 5% superior no *Recall*. A precisão de ambos os sistemas é a mesma. Além disso, o sistema proposto é capaz de superar o *OutGene* e o *Flow Hacker* em todas as métricas.

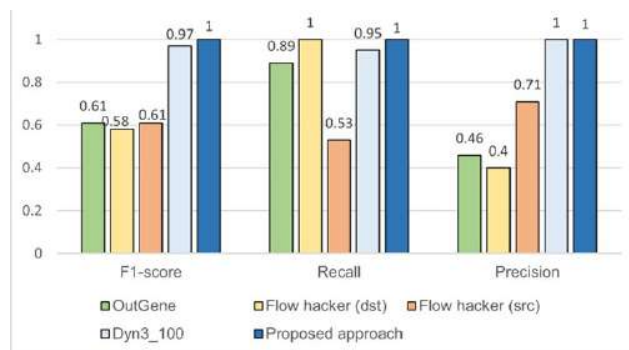


Figura 8. Comparação do desempenho da abordagem proposta (dados do anfitrião e dados da rede) com outras abordagens.

V. Conclusão e trabalhos futuros

Este trabalho mostrou as vantagens de incluir dados do anfitrião, mais precisamente, EMSWs, nos atuais SDIs. As EMSWs fornecem uma visão essencial da atividade de uma rede. Estes eventos descrevem em pormenor o funcionamento de cada máquina. Ao definir dinamicamente as SDI EMSW, foram extraídas as características mais relevantes para detetar comportamentos anómalos. A adição de características fixas que fornecem uma visão geral do comportamento das máquinas Windows é também um elemento importante

Referências

- [1] R. Hofstede et al., "Flow Monitoring Explained: From Packet Capture to Data Analysis With NetFlow and IPFIX," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2037-2064, 2014.
- [2] S. W. A. Hamdani et al., "Cybersecurity standards in the context of operating system: Practical aspects, analysis, and comparisons," *ACM Computing Surveys (CSUR)*, vol. 54, no. 3, pp. 1-36, 2021.
- [3] S. S. Soniya and S. M. C. Vigila, "Intrusion detection system: Classification and techniques," in *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, 2016: IEEE, pp. 1-7.
- [4] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16-24, 2013.
- [5] L. Dias, S. Valente, and M. Correia, "Go with the flow: Clustering dynamically-defined netflow features for network intrusion detection with DynIDS," in *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, 2020: IEEE, pp. 1-10.



Distribuição Quântica de Chaves Portátil em Espaço Livre e Alta Velocidade

Alferes-Aluno Tm Ricardo Ferreira

TPO Transmissões

Resumo - Com o surgimento da computação quântica, a criptografia clássica não é suficientemente confiável para proteger informações sensíveis. No entanto, existem alternativas. *Quantum Key Distribution* (QKD) é um método para garantir a comunicação com base nas leis da física quântica. Nesta dissertação, propõe-se uma configuração de QKD de alta velocidade em espaço livre, com o objetivo de implementar a variante de três estados de polarização um *decoy do protocolo* BB84. Uma avaliação do melhor tipo de díodo laser a ser utilizado para QKD em espaço livre é realizada entre várias opções. O desempenho do sistema foi avaliado, incorporando uma análise quantitativa das perdas do sistema e estimando o número de fótons que atravessam o canal quântico.

O sistema alcançou uma *Quantum Bit Error Rate* (QBER) de 1.58% para a base Z e 1.46% para a base X. Medidas preliminares de QBER também foram realizadas no contexto de protocolos quânticos de comunicação privada sem chave, com foco no número médio de fótons por pulso.

I. Introdução

O evoluínte campo da computação quântica tem o potencial de facilitar o acesso a dados encriptados convencionalmente, o que significa que quebra alguns protocolos criptográficos modernos. Isto levanta preocupações quanto à segurança na transferência de dados e constitui um problema que precisa ser abordado o mais rapidamente possível.

A física quântica é conhecida por possuir leis contra-intuitivas que descrevem o comportamento da matéria e energia nos níveis atômico e subatômico. Por exemplo, as medições causam perturbações, sendo impossível realizar uma medida sem perturbar um sistema quântico (exceto se o estado quântico for compatível com a medição) [1]. Esta é a base da criptografia quântica e um dos conceitos fundamentais que garantem a segurança de *Quantum Key Distribution* (QKD). Com base na ideia de que uma medição pode alterar o estado de um sistema, é possível detetar potenciais ouvintes, o que leva a QKD ser um método seguro de distribuição de chaves [2].

O objetivo deste trabalho experimental é desenvolver um sistema de comunicação de QKD em espaço livre, que será posteriormente miniaturizado e projetado para se adequar a um nanossatélite, como por exemplo, um *CubeSat*.

II. Estado da Arte

A. Sistemas Criptográficos Assimétricos e Simétricos

Os sistemas criptográficos assimétricos utilizam um par de chaves para a encriptação e desencriptação. Uma chave pública é usada para encriptar a mensagem, enquanto outra chave, denominada chave privada, é usada para desencriptá-la. Esta chave pública é obtida por meio de uma função unidirecional aplicada à chave privada e é divulgada a qualquer indivíduo interessado. A segurança destes sistemas criptográficos baseia-se na complexidade computacional (quão difícil é inverter a função unidirecional) [1]. Os computadores quânticos representam uma ameaça a esses sistemas porque permitem a realização de cálculos matemáticos exponencialmente mais rápidos do que computadores clássicos.



Em contraste, os sistemas criptográficos simétricos usam a mesma chave tanto para encriptação quanto para descriptação. Isso significa que a mesma chave tem que compartilhada entre o remetente e o destinatário para que a mensagem seja transmitida de forma segura. Esses sistemas são baseados em *one-time pads*, uma chave aleatória que deve ser tão longa quanto a mensagem e é usada apenas uma vez para encriptar ou descriptar uma única mensagem. Os *one-time pads* são teoricamente inquebráveis (comprovados seguros) uma vez que a chave é aleatória e usada apenas uma vez [3].

Os algoritmos de QKD têm como objetivo fornecer uma maneira de enviar uma chave de forma segura por meios confiáveis da Alice para o Bob, permitindo que canais inseguros compartilhem chaves arbitrariamente longas.

Dentro da matriz de informação e computação quântica, a capacidade dos computadores quânticos processarem certos tipos de cálculos exponencialmente mais rápido do que os computadores clássicos baseia-se na sua unidade fundamental de informação, o qubit.

B. Bits Quânticos, Superposição e Polarização da Luz

O qubit, um análogo quântico ao bit clássico, serve como a base dos sistemas de processamento de informação quântica, possibilitando operações seguras e complexas para além das capacidades clássicas. Na computação clássica, um bit existe num de dois estados discretos: 0 ou 1. Porém, os qubits operam sob o princípio de superposição, permitindo-lhes ocupar uma combinação linear destes estados. Matematicamente, o estado puro de um qubit $|\psi\rangle$ pode ser representado por:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (1)$$

onde $|0\rangle$ e $|1\rangle$ denotam dois estados de base ortonormal, e α e β são coeficientes complexos que descrevem amplitudes probabilísticas. Assim sendo, uma medição realizada sobre um sistema quântico perturba a sua superposição, resultando no colapso probabilístico para um dos estados de base.

No domínio da comunicação e criptografia quântica, a escolha óbvia para uma implementação física de qubit é a polarização de fótons, devido à sua elevada fidelidade, fácil manipulação e capacidade de transmissão a longas distâncias.

C. BB84

Em 1984, Bennett e Brassard introduziram QKD [4], um método no qual os estados de polarização de fótons individuais são utilizados para codificar bits de uma chave criptográfica. As medições efetuadas destes estados são definidas probabilisticamente, conforme representado por (2).

$$|\psi\rangle = \sin(\alpha)|H\rangle + \cos(\alpha)|V\rangle$$

Quando sujeito a uma medição na base rectilinear, um fóton torna-se polarizado verticalmente ou horizontalmente com probabilidades $(\sin(\alpha))^2$ e $(\cos(\alpha))^2$, respetivamente. Estes resultados derivam do estado puro de um qubit (1), após admitir que $|H\rangle$ e $|V\rangle$ representem os dois estados de base do mesmo, com $\alpha \in [0, 2\pi[$ sendo α o ângulo de polarização predominante.



O protocolo ocorre da seguinte forma:

1. A Alice inicia o processo ao enviar para o Bob uma sequência de fótons. Os fótons devem ser primeiro polarizados aleatoriamente para assumir os estados $|H\rangle$, $|V\rangle$, $|D\rangle$ ou $|A\rangle$ (0, 90, 45, -45 graus). Em seguida, o Bob recebe estes fótons pelo canal quântico e, para cada um, decide aleatoriamente se vai utilizar uma base retilinear (distinção horizontal-vertical) ou uma base diagonal (distinção diagonal-anti-diagonal) para a medição;

2. O Bob depois utiliza então um canal público para anunciar, para cada fóton, o tipo de medição que realizou, mas não o resultado obtido. A Alice também terá que confirmar ou negar publicamente se cada base anunciada pelo Bob corresponde à mesma base usada para codificar os fótons;

3. Reconciliação de bases: o Bob descarta as medições efetuadas com uma orientação diferente daquela que a Alice escolheu e mantém as restantes. Cada medição mantida representa resultados perfeitamente correlacionados com os da Alice.

4. O Bob, por último, atribui os valores binários 0 aos estados $|H\rangle$ e $|D\rangle$, e 1 aos estados $|V\rangle$ e $|A\rangle$. Após a reconciliação de bases, esta sequência de bits com metade do tamanho é chamada de *shifted key* e pode ser utilizada para codificar e decodificar uma única mensagem. "Nem Alice nem Bob podem decidir qual chave resulta do protocolo. Na verdade, é a junção das escolhas aleatórias de ambos que produz a mesma" [1].

Este protocolo é exemplificado tabela 1, na qual, Z e X simbolizam as bases retilínea e diagonal, respetivamente, enquanto S e N indicam respostas afirmativas e negativas durante o processo de reconciliação de bases.

TABELA 1
PROTOCOLO BB84

Bit aleatório da Alice	0		0		1		1	
Base aleatória da Alice	Z		X		X		Z	
Polarização do fóton enviado	$ H\rangle$		$ D\rangle$		$ A\rangle$		$ V\rangle$	
Escolha de base do Bob	Z	X	Z	X	Z	X	Z	X
Resultado da medição do Bob	$ H\rangle$	$ D\rangle, A\rangle$	$ H\rangle, V\rangle$	$ D\rangle$	$ H\rangle, V\rangle$	$ A\rangle$	$ V\rangle$	$ D\rangle, A\rangle$
Reconciliação de Bases	S	N	N	S	N	S	S	N
Chave Secreta	0			0		1	1	

III. Indicador de Desempenho

A. Quantum Bit Error Rate

Na comunicação quântica, o *Quantum Bit Error Rate* (QBER) é uma métrica vital para avaliar a fiabilidade e segurança do canal de transmissão. É definida como a razão entre o número de bits que contêm erros e o número total de bits transmitidos e recebidos. Contagens de fótons mais elevadas geralmente reduzem o QBER, mas introduzem falhas de segurança devido à presença eventos de fótons múltiplos.



As duas principais causas que afetam o aumento do QBER são as eficiências quânticas dos módulos de contagem de fótons individuais e a taxa de *dark counts*. Para quantificar o efeito desses fatores, é possível relacionar a taxa média de recepção de fótons com o número de *dark counts* de um detector. A Figura 1 ilustra esta relação.

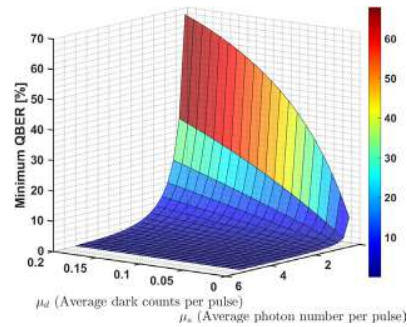


Figura 1: QBER mínimo como função dos *dark counts* e do número médio de fótons.

IV. Configuração Proposta para QKD

A. Configuração Proposta

Neste trabalho, é implementado o protocolo BB84 de três estados de polarização um *decoy* [5]. Além disso, a proposta original de [5] é simplificada, reduzindo o número de componentes no lado do emissor, tornando assim o sistema mais compacto (na perspectiva de QKD em nanossatélites).

Pulsos coerentes fracos foram o método utilizado para a criação de estados quânticos neste trabalho, sendo pulsos de luz com baixa intensidade e longa duração, podendo ser gerados utilizando lasers altamente atenuados.

A frequência dos fótons é uma variável crucial em QKD de satélite-terra. Operar na primeira janela de telecomunicações (800-900 nm) oferece diversas vantagens como a baixa absorção de fótons [6] e detectores baseados em silício bem desenvolvidos.

Como fonte de luz para gerar pulsos coerentes fracos, propõe-se o uso de díodos laser emissores de superfície com cavidade vertical (VCSEL) devido à sua alta fiabilidade e baixa dependência da temperatura nos comprimentos de onda emitidos.

B. Desempenho dos díodos VCSEL

A dispersão da luz dos díodos VCSEL no espaço livre é uma métrica fundamental no âmbito de QKD de longa distância e pode ser avaliada analisando o diâmetro gaussiano que corresponde ao tamanho do feixe num ponto específico da sua propagação, particularmente onde a intensidade é $1/e^2$ (ou cerca de 13.5%) da intensidade máxima. Este diâmetro é usado para caracterizar a qualidade do feixe do laser e prever o comportamento do mesmo à medida que se propaga. Os díodos VCSEL apresentaram alta divergência em espaço livre, resultando em perdas significativas de potência devido ao feixe exceder as aberturas de recepção de fótons.

Com o objetivo de melhorar esta divergência, foi acoplada a saída de díodos laser a fibras óticas para limpar a largura espectral dos feixes, uma vez que fibra ótica permite a criação de um feixe com uma distribuição espacial ideal na forma de uma Gaussiana. Após esta implementação, a divergência foi reduzida por um fator de 14 para o eixo X (de 2.62 para 0.18 miliradianos).



C. Preparação dos Estados

Para a implementação do protocolo 3 estados 1 *decoy*, é necessário induzir polarização para a criação da chave criptográfica. Os três estados necessários são horizontal, vertical e diagonal. Os estados reticulíneos horizontal e vertical (base Z) são usados para criar a shifted key, enquanto o estado diagonal (base X) é criado exclusivamente com o objetivo de detetar potenciais ouvintes.

Após a geração de pulsos polarizados, o pulso laser precisa de ser suficientemente atenuado para controlar o número médio de fótons emitidos e, consequentemente, controlar a segurança com a qual os estados estão a ser transmitidos.

D. Medidas de Polarização

No receptor, os pulsos recebidos são divididos em duas trajetórias para medições nas bases Z e X, de forma aleatória. Para facilitar a diferenciação entre as medições realizadas nessas duas bases durante o pós-processamento, é introduzido um atraso temporal na trajetória da base X. O atraso é induzido colimando este feixe em 1590 metros de fibra ótica monomodo, tornando-o discernível e facilmente isolável computacionalmente.

Para distinguir entre polarizações horizontal e vertical na projeção da base Z, é implementado um cubo *Polarizing Beamsplitter* (PBS). Fótons polarizados horizontalmente atravessam este cubo e são posteriormente colimados num módulo de contagem, os fótons polarizados verticalmente são refletidos e direcionados para outro módulo de contagem. O cubo PBS utilizado para as medições de polarização na base Z é reaproveitado para efetuar medições na base X, após a introdução de uma mudança de fase.

Utilizando um par de módulos de contagem de fótons, a configuração é ajustada para detectar fótons recebidos e, assim, discriminar estados de polarização ao longo das bases reticulíneas e diagonais.

V. Resultados

A. Atraso da base ortogonal

A estimativa do atraso temporal no pós-processamento foi realizada ao colimar a trajetória da base X numa fibra ótica monomodo, fazendo assim com que os fótons percorram um caminho mais longo e atinjam o detector com um atraso. Com base em índices de refração típicos para fibras de 850 nm, um atraso estimado de 8,4 μs foi calculado para a fibra de 1590 metros utilizada. A Figura 2 representa o atraso médio na detecção de fótons após o pulso de ligação do díodo VCSEL. Aplicando um ajuste gaussiano de dois parâmetros, é possível determinar o atraso médio de ambas as distribuições gaussianas que atingem o mesmo módulo de contagem, conforme feito em (3).

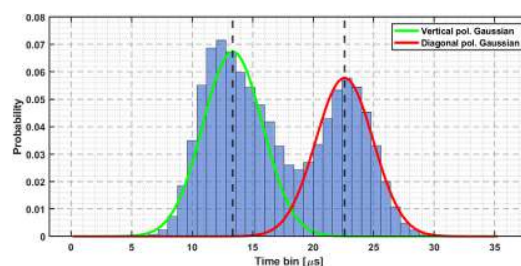


Figura 2: Atraso temporal observado entre as polarizações vertical e diagonal.



$$atraso = 22.6 \times 10^{-6} - 13.3 \times 10^{-6} = 9.3\mu s$$

Com um atraso temporal característico de aproximadamente 9,3 μs , a frequência ótima para a discriminação de polarização é aquela que se alinha com o término da emissão do VCSEL, coincidindo assim com a chegada dos fótons atrasados aos detectores. Além disso, o detector ativo neste intervalo específico determina o resultado da medição de polarização.

B. Perdas

A eficácia de um sistema de QKD está intrinsecamente ligada às perdas acumuladas em várias etapas de sua operação. Uma análise quantitativa dessas perdas é indispensável para avaliar o desempenho geral e a fiabilidade do sistema (tabela 2).

TABELA 2
PERDAS PARA O CASO MÉDIO E PIOR CASO

	Caso Medio [dB]	Pior Caso [dB]
Emissor	11.2	11.6
Espaço Livre	0.6	0.7
Recetor	15.1	17.0

C. Estimação do número médio de fótons emitidos e recebidos

A determinação da contagem média de fótons que atinge o detector é crucial para manter uma baixa taxa de emissão. A relação entre o número de fótons que atingem os detetores e a densidade ótica introduzida, é ilustrada de forma detalhada na Fig. 3.

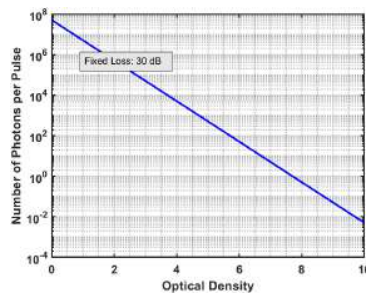


Figura 3: Relação entre densidade ótica e o número médio de fótons por pulso

Uma vez que o número de fótons é linearmente dependente da potência ótica, a razão de fótons entre o emissor e o receptor pode ser definida como R_p :

$$R_p = \frac{N_{emissor}}{N_{recetor}} = \frac{P_{emissor}}{P_{recetor}} = 10^{\frac{C_{perdas}}{10}}$$

Para uma perda no canal quântico para o detetor de 17,7 dB, a razão de fótons R_p é aproximadamente 59,16. Deste modo, a relação entre as contagens médias típicas de fótons que chegam ao detetor e aquelas emitidas pela fonte assume este valor para o pior caso, fornecendo uma medida quantitativa da eficiência do canal de transmissão.



D. Quantum Bit Error Rates

Devido a uma alta taxa média de *dark counts* de 0,06 por pulso a 50 kHz nos módulos de contagem utilizados, uma média de fótons por pulso muito baixa não é viável. Tal cenário resultaria num QBER proibitivamente alto de 37,0% para 0.1 fótons por pulso (média usada em configurações atuais), muito além do limite aceitável de 3,5% para protocolos BB84 com estados de decoy [7]. Consequentemente, torna-se imperativo manter uma taxa média de detecção de fótons de pelo menos 1 por pulso para garantir que o QBER permaneça abaixo do limite superior estipulado.

O QBER na base Z (tabela 3) foi avaliado utilizando um PBS para separar fótons com polarizações horizontal e vertical. Como os estados quânticos foram criados alternadamente, o método mais direto para calcular o QBER envolve avaliar as contagens de fótons em cada detector em cada pulso emitido pelo VCSEL.

O QBER da base X foi realizada de forma semelhante; no entanto, os estados criados foram polarizações diagonal e anti-diagonal, com uma diferença de fase introduzida no receptor para distinguir efetivamente esses estados quânticos. O QBER medido para a base X é apresentado na tabela 4.

TABELA 3
QBER NA BASE Z

	$QBER_z$
N=2	1.58%

TABELA 4
QBER NA BASE X

	$QBER_x$
N=2	1.46%

É essencial notar que a configuração experimental empregada nesta dissertação serve como uma prova de conceito preliminar. Futuro trabalho visa a utilização de equipamentos mais eficientes assim como a miniaturização da configuração existente para uma integração eventual num sistema de comunicação baseado num *CubeSAT*.

VI. Conclusão

Resumindo, este trabalho fornece uma análise aprofundada de QKD em espaço livre, com foco na geração de pulsos coerentes fracos, divergência do feixe utilizado e modelos estatísticos para probabilidades de eventos. Díodos laser de superfície emitente vertical foram identificados como fontes ótimas, embora com algumas perdas de colimação. Um QBER de 1.58% foi atingido para a base Z e 1.46% para a base X, enfatizando o impacto dos *dark counts* nestes resultados. Também foram realizadas medições de erros para protocolos preliminares de comunicação privada quântica sem chave. Em geral, o trabalho efetuado culmina em conceitos teóricos e práticos cruciais para a implementação de protocolos de QKD e a sua melhoria.

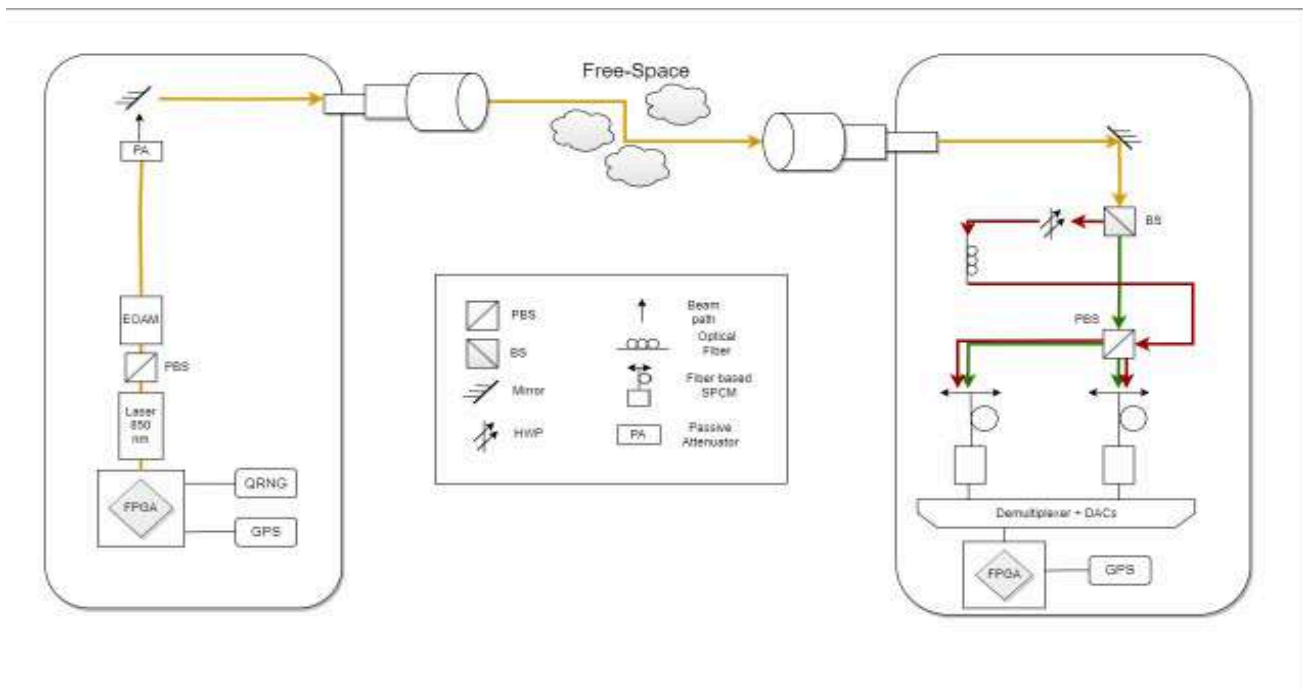


Figura 4: Ilustração do esquema experimental

Bibliografia

- [1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, Mar. 2002.
- [2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014.
- [3] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
- [4] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing (Proceedings of IEEE International Conference on Computers, Systems & Signal Processing)*. Bangalore, India: Steering Committee, Dec. 1984.
- [5] F. Grunefelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Simple and high-speed polarization-based QKD," *Applied Physics Letters*, vol. 112, no. 5, p. 3, Jan. 2018.
- [6] V. Fernandez, K. J. Gordon, R. J. Collins, et al., "Quantum key distribution in a multi-user network at gigahertz clock rates," in *Photonic Materials, Devices, and Applications*, G. Badenes, D. Abbott, and A. Serpenguzel, Eds., Sevilla, Spain: SPIE, Jul. 2005.
- [7] A. Jain, A. Khanna, J. Bhatt, P. V. Sakhiya, and R. K. Bahl, "Experimental demonstration of free space quantum key distribution system based on the BB84 protocol," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kharagpur, India: IEEE, Jul. 2020.



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

