ISSN25943952

O Comunicante

SUMÁRIO

Artigos

Revista Científica da Escola de Comunicações
Escola Coronel Hygino Corsetti

VOLUME 11 - N° 1
Dezembro 2021

ISSN25943952

SUMÁRIO

Artigos

VOLUME 11 - N°1
Dezembro 2021

Volume 11 - N° 1
Dezembro 2021
ISSN 1968-6029
ISSN 2594-3952 (Digital)
Escola de Comunicações - EsCom
Escola Coronel Hygino Corsetti

EDITORIAL

Esta edição da Revista Científica O Comunicante reveste-se de especial importância, tendo em vista sua publicação no ano em que a Escola de Comunicações (EsCom) completou seu primeiro centenário. Desde 1921, a EsCom vem transmitindo conhecimentos relevantes para a Arma do Comando e contribuindo, desta forma, para a operacionalidade da Força.

Nos últimos 30 anos, houve mais desenvolvimento científico e tecnológico do que no século passado. Televisores de alta resolução, mídias de armazenamento cada vez menores e com mais espaço, processadores e chips complexos, GPS e smartphones são alguns exemplos da tecnologia que empregamos no nosso dia a dia e que influenciam nas Comunicações e na Cibernética.

A agilidade dos acontecimentos torna o que aprendemos hoje desatualizado e obsoleto amanhã. Por isto, devemos pensar à frente, buscar dominar não somente a tecnologia que empregamos, mas o que se tem de mais moderno no momento e o que se pretende para o futuro. É nessa empreitada que a Revista Científica da EsCom se lança, no intuito de publicar artigos técnicos e informativos, elaborados por docentes, discentes e colaboradores externos à Escola.

Esta edição atual reforça o compromisso da Escola Coronel Hygino Corsetti com a inovação, o planejamento, o autoaperfeiçoamento e a capacitação continuada, buscando aguçar e desenvolver o interesse dos leitores em diversas áreas de conhecimento, tais como Cibernética, Ciência e Tecnologia, Doutrina, Educação, História Militar, Informática, Gestão e Operações Militares.

O Comando da EsCom agradece a contribuição de todos que submeteram os artigos para análise e aproveita para convidar o público entusiasta a contribuir com trabalhos acadêmicos nas futuras edições desta revista.

Uma boa leitura a todos.

Cel Sandro Silva Cordeiro
Comandante da Escola de Comunicações

EXPEDIENTE

A Revista Científica O Comunicante, publicada pela Escola de Comunicações, busca incentivar pesquisas científicas nas áreas afetas à Defesa e que contribuam para o desenvolvimento da Arma de Comunicações.

OBJETIVOS

Promover o viés científico em áreas do conhecimento que sejam de interesse da Arma de Comunicações e, consequentemente, do Exército Brasileiro.

Manter um canal de relacionamento entre o meio acadêmico militar e civil.

Trazer à reflexão temas que sejam de interesse da Força Terrestre e que contribuam para a Defesa.

Publicar artigos inéditos e de qualidade.

Aprofundar pesquisas e informações sobre assuntos da atualidade em proveito da Defesa e difundir aos corpos de tropa.

PÚBLICO-ALVO

A revista está voltada a um amplo espectro de pesquisadores, professores, estudantes, militares, bem como profissionais que atuem nas áreas de Defesa, Cibernética, Ciência & Tecnologia, Direito Militar, Doutrina, Educação, Informática, História Militar, com ênfase em Comunicações e Equipamentos de Comunicações, Instrução Militar, Gestão, Meio Ambiente, Operações Militares Conjuntas e Singulares.

PUBLICAÇÃO DE ARTIGOS

Os artigos apresentados para submissão devem ser livres de embaraços. Caso o autor tenha submetido o Artigo a outra revista, ele deverá consultá-la e certificar-se de não estar ferindo direitos de publicação conferidos à revista anterior.

PROCESSO DE AVALIAÇÃO

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

Em seguida, os textos são encaminhados aos pareceristas que terão o prazo de 30 dias para fazerem a avaliação. Os pareceristas não são remunerados e, caso aceitem participar, terão seus nomes incluídos no Comitê de Avaliadores, publicados a cada volume da revista. A partir das avaliações dos pareceristas, o Comitê Editorial pode decidir editar ou não os artigos submetidos, além de sugerir mudanças eventuais de modo a adequar os textos.

Os textos submetidos devem vir acompanhados de carta de autorização para publicação que garantirá seu ineditismo ou, ainda, que apesar de estar concorrendo a publicação em outras revistas, não está ferindo direitos de publicação com terceiros para ser veiculado nesta revista.

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

PERIODICIDADE

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

O Comunicante - Revista Científica da Escola de Comunicações - Volume 11, N° 1 (Dez/2021)
Brasília-DF: Escola de Comunicações. 2021 88p; 29,7 cm X 21,0 cm
Publicação Anual
ISSN 1968-6029 ISSN 2594-3952 (Digital)
Revista Científica da Escola de Comunicações
1. Escola de Comunicações 2. Defesa 3. Cibernética 4. Ciência & Tecnologia 5. Doutrina 6. Direito 7. Educação 8. Informática 9. Instrução Militar 10. Gestão 11. Meio Ambiente 12. Operações Militares Conjuntas e Singulares.

ARTIGO CIENTÍFICO

ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

PROPOSTA DE EMPREGO DO SISTEMA DE AERONAVES REMOTAMENTE PILOTADAS COMO PLATAFORMA DE OPTRÔNICOS NAS AÇÕES DE RECONHECIMENTO, VIGILÂNCIA E AQUISIÇÃO DE ALVOS.

PAULO DE AQUINO LOPES FILHO
AUGUSTO DA SILVA GUIMARÃES

RESUMO: Este trabalho tem como objetivo propor, considerando vantagens e desvantagens de cada tipo de equipamento, os tipos ideais de optrônicos que podem estar presentes em uma ARP (Aeronaves Remotamente Pilotadas) para a realização das ações de Reconhecimento, Vigilância e Aquisição de alvos. Para tanto, este Trabalho de Conclusão de Curso foi desenvolvido por meio de uma pesquisa bibliográfica documental, do tipo qualitativa, que contemplou leitura analítica e fichamento das fontes, argumentação e discussão de resultados. A pesquisa bibliográfica permitiu o aprofundamento nos principais tópicos em questão, dentre eles: optrônicos, inteligência e onde constam as ações de RVA com os respectivos SARP e optrônicos ideais para sua realização. SARP. Chegou-se assim ao objetivo explicitado, sendo produzido como resultado final uma tabela onde constam as ações de RVA com os respectivos SARP e optrônicos ideais para sua realização.

Palavras Chaves: SISTEMA DE AERONAVES REMOTAMENTE PILOTADAS. AERONAVE REMOTAMENTE PILOTADA. INTELIGÊNCIA. OPTRÔNICOS. RECONHECIMENTO, VIGILÂNCIA E AQUISIÇÃO DE ALVOS.

1. INTRODUÇÃO

Segundo o manual de campanha EB20-MC-10.207 - Inteligência (2015), os combates modernos têm se caracterizado pelo intenso uso de tecnologia, velocidade e letalidade seletiva, assim como pela utilização de ARP (aeronaves remotamente pilotadas).

Nesse novo cenário, têm-se constatado que a função de combate Inteligência influencia todas as outras funções de combate, por serem diretamente afetadas ou relacionadas com os produtos da inteligência. Isso tem levado vários países a intensificar o desenvolvimento da função de combate inteligência (BRASIL, 2015), a qual busca assegurar compreensão sobre o ambiente operacional, as ameaças (atuais e potenciais), os oponentes, o terreno e as considerações civis.

Com base no que é determinado pelo Comandante, a função de combate Inteligência executa tarefas associadas à Inteligência Militar Terrestre propriamente dita, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA).

As ações de Reconhecimento e Vigilância, comuns a todas as operações, são realizadas geralmente por meio do emprego de meios (pessoal e material) militares para coletar ou buscar e/ou verificar dados ou informações e/ou conhecimentos que servirão de matéria prima para a etapa da produção de Inteligência nas operações terrestres. (BRASIL, 2014)

Segundo o manual EB70-MC-10.214 (Vetores Aéreos da Força Terrestre), importantes plataformas que realizam as supracitadas ações com segurança, eficiência, discrição e rapidez são as ARP, as quais podem carregar sensores dos mais diversos tipos, sejam para atividades de guerra eletrônica de comunicações ou não comunicações.

As ARP cresceram de importância nos últimos anos, justamente devido a suas possibilidades de uso, que vão desde entretenimento a empregos militares. No uso militar, percebe-se o quanto esse segmento é crescente, por exemplo, no ano de 2012, as Aeronaves Remotamente Pilotadas

correspondiam a mais de 31% da frota militar dos Estados Unidos, sendo um negócio em franca expansão (JULIBONI, 2012).

Algumas ARP de grande porte, como o RQ-4 Block 40 Global Hawk da Northrop Grumman Global podem carregar sistemas militares-específicos, como radares SAR (abertura sintética), sensores eletro-ópticos/ infravermelhos de longo alcance com ótima resolução, câmeras e outros, sendo perfeitamente capazes de ações de Reconhecimento, Vigilância e Aquisição de Alvos (SAYLER, 2015).

Diante do exposto, infere-se que o domínio da técnica e tática relativas à utilização dos SARP como plataformas de RVA é importante nos dias de hoje para a eficiência do ciclo de inteligência, especialmente na fase de obtenção.

2. DESENVOLVIMENTO

2.1 PROBLEMA

O manual de fundamentos da Inteligência Militar Terrestre, EB20-MF-10.107 (2015), cita que a inteligência militar, em qualquer nível de atuação, possui um objetivo comum: a permanente identificação das ameaças, minimizando incertezas e buscando oportunidades para o sucesso das operações. O uso de plataformas eficientes para RVA precisa ser prioridade para que a obtenção de dados de interesse seja mantida e os sensores optrônicos embarcados em aeronaves remotamente pilotadas podem ser responsáveis por boa parte desses dados. Posto isso, considerando vantagens e desvantagens de cada tipo de equipamento, quais os tipos ideais de optrônicos que podem estar presentes em uma ARP para a realização das ações de RVA?

2.2 OBJETIVOS

A solução do problema supracitado se constitui na consecução do objetivo geral desta pesquisa, que pode ser formalizado através da proposta de um emprego eficiente para o Sistema de Aeronaves Remotamente Pilotadas (SARP) como plataforma de optrônicos nas ações de RVA. A fim de viabilizar a consecução do objetivo geral de estudo, foram estabelecidos os seguintes objetivos específicos:

- Caracterizar a função de combate inteligência, assim como suas tarefas e atividades;
- Conhecer os objetivos das ações de Reconhecimento, Vigilância e Aquisição de Alvos;
- Conhecer as características e tecnologias empregadas nos combates modernos, no que tange às ações de Reconhecimento, Vigilância e Aquisição de Alvos;
- Conhecer os tipos e características das ARP atuais;
- Conhecer as vantagens e desvantagens dos diversos tipos de optrônicos que podem ser embarcados em ARP para realização de tarefas de reconhecimento, vigilância e aquisição de alvos;

2.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

Segundo o Manual de Campanha EB20-MC-10.207, Função de Combate Inteligência (2015), a Função de Combate Inteligência funciona como integradora entre os elementos essenciais do poder de combate, juntamente com as informações e a capacidade de liderança e comando e controle do comandante. Esses elementos não podem ser dissociados e são vitais para o preparo e emprego da F Ter no cumprimento de suas missões.

A capacidade que as diferentes categorias de ARP possuem de transportar diversos tipos de sensores, com diferentes características físicas e operacionais, deve ser explorada para aumentar a eficiência do ciclo de comando e controle, pois através do C2 e Informações todas as funções de combate têm a eficiência aumentada.

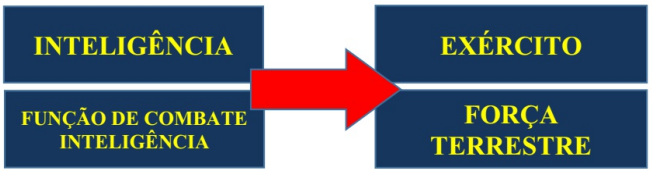
2.4 A FUNÇÃO DE COMBATE INTELIGÊNCIA

O Manual de Campanha EB20-MC-10.207 (2015) cita que as funções de combate são um conceito, um instrumento que agrupa,

descreve e coordena as atividades das forças terrestres. Torna mais fácil o planejamento e a execução das operações, além da instrução e do adestramento das unidades no nível tático.

A Inteligência, apesar de ser uma das seis funções de combate, abrange as demais funções, já que elas são afetadas ou estão relacionadas com os produtos da Inteligência.

FIGURA 1: Relações da Inteligência e função de combate inteligência



Fonte: BRASIL, 2015, p. 2-1. (EB20-MC-10.207)

Em particular, as funções de Comando e Controle e Proteção englobam atividades e tarefas próprias do Sistema de Inteligência do Exército (SIEx).

A Função de Combate Inteligência executa tarefas associadas às operações de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA), de acordo com as diretrizes do Comandante, normalmente traduzidas em Necessidades de Inteligência (NI). (BRASIL, 2015).

2.4.1 AS AÇÕES DE IRVA E SEUS OBJETIVOS

O objetivo das ações de IRVA é fornecer informações oportunas, precisas e relevantes de dados de Inteligência para todos os níveis de comando. A idéia é apoiar o comandante com o máximo de informações úteis para suas decisões. Nas operações militares, particularmente no nível tático, o comando requer informações com precisão, em tempo real, sobre o inimigo (LAZARO, 2015).

2.5 OS SARP ATUAIS

Segundo Almeida (2009), os Sistemas de Aeronaves Remotamente Pilotadas foram concebidos e construídos para serem usadas em missões muito perigosas ao emprego do ser humano, nas áreas de Inteligência militar, apoio aéreo a tropas de infantaria e cavalaria no campo de batalha, apoio e controle de tiro de artilharia, controle de mísseis de cruzeiro, patrulhamento urbano, costeiro, ambiental e de fronteiras, atividades de busca e resgate, entre outras.

VANT é abreviação de Veículo Aéreo Não Tripulado, nomenclatura em português correspondente à sigla UAV em inglês (Unmanned Aerial Vehicle), adotada pelo Departamento de Defesa Norte Americano (Department of Defense - DoD).

Com o desenvolvimento da tecnologia, os VANT ficaram cada vez mais versáteis, letais e com maior autonomia. Um exemplo disso é o já citado VANT americano RQ-4 Global Hawk, com um raio de ação de 22.780 km, chegando a 60.000 pés, podendo transportar 1.360 kg de material e permanecendo em voo por até 36 horas. (NETO; ALMEIDA, 2009, p. 19-21).

O manual EB70-MC-10.214 (Vetores Aéreos da Força Terrestre) define o Sistema de Aeronaves Remotamente Pilotadas como:

“conjunto de meios necessários ao cumprimento de determinada tarefa com emprego de ARP, englobando, além da plataforma aérea, a carga paga (payload), a estação de controle de solo, o terminal de transmissão de dados, terminal de enlace de dados, a infraestrutura de apoio e os recursos humanos. Em função do desenvolvimento tecnológico, alguns desses componentes podem ser agrupados.”

Assim, pode-se definir o SARP, basicamente, como uma plataforma operada remotamente por um controle em terra ou que segue um plano de voo pré-estabelecido antes de seu lançamento, capaz de executar diversas tarefas, tais como reconhecimento tático, monitoramento, vigilância, ataque e mapeamento, entre outras, dependendo dos equipamentos instalados. (OLIVEIRA, 2005).

2.5.1 CLASSIFICAÇÃO DOS SARP

Os principais parâmetros para a classificação dos SARP são: desempenho, a massa (peso) do veículo, a natureza das ligações utilizadas, os efeitos produzidos pela carga paga (compreende os sensores e equipamentos embarcados na plataforma aérea, que permitem o cumprimento das missões), as necessidades logísticas ou o escalão responsável pelo emprego do sistema.

O Manual de Campanha EB70-MC-10.214 (Vetores Aéreos da Força Terrestre) diz que o nível do elemento de emprego é a principal referência para a definição das categorias, conforme descrito no quadro a seguir:

QUADRO 1 – Classificação e categorias dos SARP para a Força Terrestre

Grupo	Categoria (Cat)	Elemento de Emprego	Nível de Emprego
III	5	MD/EMCFA	Estratégico
	4	C Cj	Operacional
II	3	CEx/DE	Tático
I	2	DE/Bda	
	1	Bda/U	
	0	até SU	

Fonte: BRASIL, 2020, p. 4-5. (EB70-MC-10.214)

a) **Categorias 0 (zero) a 1 (um)** - transportados em mochilas e preparados, operados e lançados por equipes de 01 (um) a 02 (dois) homens;

FIGURA 2: Exemplo de operação de SARP cat 1

Fonte: BRASIL, 2014, p. 4-6. (EB20-MC-10.214)

b) Categoria 2 (dois) - operados a partir de uma ou mais viaturas, mesmo que decole a partir de pistas ou outros locais não preparados ou com pouca preparação. Requer uma equipe de até 05 (cinco) homens para o seu transporte, preparo, operação e lançamento. As categorias de 0 a 2 são eficazes na vigilância de estruturas estratégicas e pontos isolados do Teatro de Operações/Área de Operações. São sensores eficazes para monitoramento de áreas de interesse, os quais, quando integrados a softwares de análise de padrões, permitem o alerta antecipado do escalão decisor. (BRASIL, 2020)

c) Categorias 3 (três) e superiores - operados a partir de aeródromos ou locais preparados, precisando de transporte para fim de translado. Demanda uma equipe de mais de 05 (cinco) homens para o transporte, preparação, operação, apoio de solo e suporte logístico. Os SARP de categoria 3 permitem realizar vigilância de largas frentes com eficácia, papel que é muito importante pois proporciona alerta antecipado e economiza os recursos disponíveis. (BRASIL, 2020).

Tomando por base as características supramencionadas, infere-se os seguintes pontos positivos para o emprego de ARP:

1. Não há a exposição de tripulação humana aos riscos de uma operação militar;
2. Os optrônicos embarcados ampliam a eficiência das ações de reconhecimento, vigilância e aquisição de alvos;
3. A capacidade de carga que não é empregada para o transporte de uma tripulação humana pode ser convertida em mais equipamentos para emprego na missão de reconhecimento, vigilância e aquisição de alvos;
4. Há um gasto menor de recursos com o emprego de ARP do que em missões com aeronaves tripuladas;
5. Os ARP podem ter uma autonomia de voo maior que aeronaves tripuladas.

Ainda, quanto aos recursos ideais que uma ARP deve apresentar para ser útil às

ações de RVA, chega-se à seguinte conclusão:

1. grande capacidade de carga para instalação de optrônicos;
2. características stealth em relação a radares;
3. grande autonomia;
4. pequenas proporções, dificultando sua visualização a olho nu.

2.6 OS PRINCIPAIS OPTRÔNICOS EMPREGADOS PARA RVA

Os sistemas optrônicos utilizam as emissões do alvo ou a energia refletida por eles na faixa óptica e cada vez mais são requisitados para aplicações militares, principalmente em sistemas de vigilância e de acompanhamento, englobando intensificadores de imagem, imageadores termais e dispositivos a LASER (CIGE, 2014).

Segundo o manual EB70-MC-10.214 (Vetores Aéreos da Força Terrestre), os SARP devem ser equipados com sensores que permitam a execução de tarefas relacionadas à obtenção de imagens (diurnas e noturnas), incluindo dispositivos de imageamento infravermelho termal e intensificadores de luminosidade ambiente. Devem possibilitar, também, georreferenciamento dos alvos. Ainda que a vigilância e o apoio ao reconhecimento sejam a vocação principal do SARP, na maioria das operações, esses sistemas podem também apoiar outras ações, tais como:

a) realização de segurança dos movimentos terrestres (tropas e comboios de suprimento);

b) proteção de estruturas estratégicas e pontos sensíveis;

c) observação aérea;

d) detecção de artefatos explosivos improvisados (AEI);

e) apoio de fogo à Força de Superfície, realizando o tiro com sistemas de armas embarcado, ou apoiando a observação e a condução do tiro

2.6.1 INTENSIFICADORES DE IMAGEM

À noite, mesmo que com baixa intensidade, existe radiação luminosa proveniente da luz das estrelas e da reflexão da luz do sol na lua e nos planetas. Na pior situação possível de luminosidade (noite sem luar e com céu encoberto) a luz residual é da ordem de 10-4 Lux (CIGE, 2014).

Os intensificadores de imagem amplificam a luminosidade do ambiente ao nível, aproximadamente, de 1 Lux (correspondente à luz crepuscular), em que os bastonetes (células da retina que convertem energia luminosa em sinais elétricos para o cérebro) começam a operar. Infere-se, então, que um dispositivo de visão noturna deverá prover um ganho de luminosidade da ordem de 10.000 vezes (ADAMY, 2004).

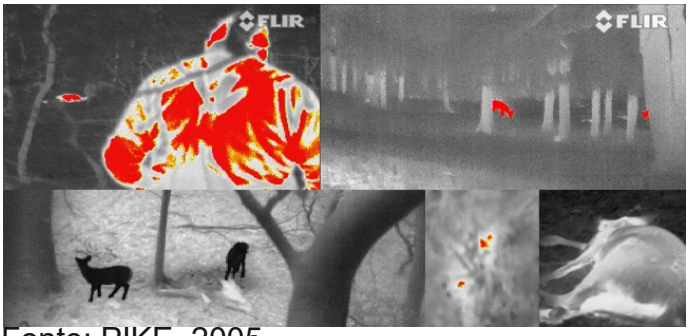
Um problema comum aos intensificadores de imagem é o aumento do nível de ruído luminoso à noite. Devido ao elevado nível de luminosidade durante o dia, suas variações tornam-se insignificantes, enquanto à noite são bastante significativas, podendo mascarar as imagens que se tenta observar por meio desse optrônico (PIKE, 2005)

2.6.2 IMAGEADORES TERMAIS

O princípio básico do funcionamento desses sensores é que todos os alvos com temperatura acima de zero grau Kelvin (°K) emitem radiação eletromagnética (REM) proporcional a sua temperatura e, predominantemente, em comprimentos de ondas (λ) na faixa do infravermelho termal (IVT), ou seja, entre 3 e 14 μm (CORADESQUE, 2014).

As imagens termais constituem um complemento para o reconhecimento visível, pois podem ser empregadas em condições nas quais o primeiro seria impossível, permitindo que imagens de alvos camuflados, submersos ou subterrâneos sejam registradas. A exemplo disso, já em 1960, as forças soviéticas empregavam técnicas por meio de sensores termais, os quais permitiam detectar submarinos a 40 m de profundidade (CIGE, 2004).

FIGURA 3: Imagem captada por imageador



Fonte: PIKE, 2005

Os detectores infravermelhos, se comparados aos intensificadores de imagem, apresentam as vantagens de conseguir observar através de camuflagem e não dependerem do nível de luminosidade ambiente (não sofrendo saturação), mas são suscetíveis às condições atmosféricas (principalmente chuva) e necessitam de muita energia e refrigeração para poderem operar, além de serem mais caros que os dispositivos de visão noturna convencionais e apresentarem maior peso e volume. (ADAMY, 2004).

Quanto aos recursos ideais que um optrônico deve apresentar para ser útil às ações de RVA, as opções foram escalonadas da seguinte forma, em ordem de importância:

1.Imageamento termal;
2.Capacidade de gravação dos fatos/ alvos monitorados;
3.Intensificação de luminosidade do ambiente;
4.Capacidade de “zoom”, facilitando a observação a alvos distantes;
5.Capacidade de medir distâncias através de telemetria a laser.

Quanto aos intensificadores de imagem, há 04 gerações de equipamentos, sendo a geração 0 (zero) a mais antiga e a geração 03 (três) a mais moderna e eficiente. O seguinte quadro foi gerado baseado nas informações adquiridas e em pesquisas bibliográficas:

Os intensificadores de imagem ficaram menores, mais eficientes e duráveis ao longo do tempo e as diferenças básicas em relação aos imageadores termais ainda se mantém: os imageadores termais não necessitam de nenhuma iluminação do ambiente, são em geral mais pesados e precisam de um sistema robusto de refrigeração.

QUADRO 2– Comparação entre as gerações de intensificadores de imagem

	G0	G1	G2	G3
Década	40	60	70	80
Ganho	800 vezes	1000 vezes	20.000 vezes	30.000 a 50.000 vezes
Vida Útil	1000 horas	2.000 horas	2.500 horas	10.000 horas
Diferenças Básicas	Necessitavam iluminação artificial	Vários estágios ou "cascatas"	Prato de Micro-canais	Foto catodo de Arsena-to de Gálio

Fonte: PIKE, 2005

QUADRO 3 – Comparação entre as gerações de intensificadores de imagem (distância de detecção).

	G2	Super G2	G3 OMNI I e II	G3 OMNI III	G3 OMNI IV	G4 (G3 OMNI VII)
Distância de detecção (m)	170	270	240	290	360	430
Porcentagem de acréscimo em relação à G2	0%	60%	40%	70%	110%	153%

Fonte: PIKE, 2005

Quanto às possibilidades e limitações dos imageadores termais em relação aos intensificadores imagem, infere-se que os imageadores termais seriam mais eficientes do que os intensificadores de imagem para RVA, porém, são equipamentos pesados, com necessidade de complexo sistema de refrigeração e alimentação, características não adequadas para emprego em ARP de pequeno porte. As ARP de grande porte como o Hermes 900 (carga útil de 300 kg) portam sistemas de imageamento termal, além de um conjunto de 10 câmeras de alta resolução, entre outros sensores, mas é importante lembrar que os custos de operação aumentam bastante nesse caso.

O custo-benefício deve ser levado em consideração. Assim, deve-se pesar, de acordo com a missão específica, quais tipos de optrônicos devem ser empregados.

3. CONCLUSÃO

A ARP, para ser empregada em ações de RVA, deve possuir características técnicas e equipamentos que a permitam cumprir a missão com maior eficácia, tais

QUADRO 4: Comparação entre intensificadores de imagem e imageadores

Imageadores Termais	**Intensificadores de Imagem**
Necessitam refrigeração	Não necessitam refrigeração
Mais pesados	Mais leves
Mais caros	Mais baratos
Não necessitam iluminação	Necessitam de mínima iluminação / São ofuscados ou saturados facilm

Fonte: PIKE, 2005

como autonomia condizente com a duração da missão e capacidade de carga que permita levar sensores de imageamento necessários (optrônicos e outros).

Dentre os recursos ideais que um optrônico deve apresentar para ser útil às ações de RVA, o imageamento termal foi tido como o mais importante, já que os equipamentos com essa capacidade não necessitam de nenhuma iluminação do ambiente. Porém, são em geral mais pesados e precisam de um sistema robusto de

refrigeração.

Outro importante ponto a se destacar é que não se deve descartar o uso de intensificadores de imagem embarcados em ARP para ações de RVA. Com seu menor peso e consumo de energia, podem ser úteis e ideais para diversas missões específicas, quando houver luminosidade mínima necessária no ambiente e ausência de fumaça ou névoa.

Como citado anteriormente, o custo-benefício deve ser sempre levado em consideração. De acordo com a missão específica, deve-se planejar quais tipos de optrônicos devem ser empregados.

Conclui-se, portanto, que as ARP são importantes plataformas para RVA, evitando em muitos casos que o ser humano se exponha aos perigos de uma operação militar para realizar essas ações. Também, é possível e desejável o emprego de optrônicos embarcados em ARP para realizar ações de RVA, tendo em vista que esses equipamentos ampliam a capacidade da visão humana, tornando o processo mais eficiente. Naturalmente, optrônicos diferentes devem ser utilizados de acordo com as necessidades de cada missão.

Como resultado, foi gerada uma tabela (Solução Prática) onde constam as ações de RVA com os respectivos SARP e optrônicos ideais para sua realização.

3.1 SOLUÇÃO PRÁTICA

A tabela abaixo pretende subsidiar o planejamento do emprego de optrônicos embarcados em ARP para ações de RVA. Neste sentido, correlacionaram-se as ações de IRVA, as tarefas

TABELA 1 – Comparação entre ações de RVA, optrônicos e ARP para esse emprego.

<table>
<tr><th>ATIVIDADE DA FUNÇÃO DE COMBATE INTELIGÊNCIA</th><th>TAREFAS RELATIVAS A ESSA ATIVIDADE</th><th>NÍVEL DE CLARIDADE DA NOITE</th><th>OPTRÔNICO INDICADO</th><th>CATEGORIA DE ARP INDICADA</th></tr>
<tr><td rowspan="8">Executar ações de IRVA</td><td>Executar sincronização e integração das</td><td colspan="3">Não é o caso</td></tr>
<tr><td rowspan="7">Conduzir reconhecimentos, vigilância, operações e missões relacionadas à inteligência e apoio na busca de alvos</td><td>Dia</td><td>Câmeras de alta definição.</td><td>0 a 6</td></tr>
<tr><td>1</td><td rowspan="3">Intensificadores de imagem</td><td>2 a 6</td></tr>
<tr><td>2</td><td></td></tr>
<tr><td>3</td><td></td></tr>
<tr><td>4</td><td rowspan="2">Imageadores termais</td><td rowspan="2">4 a 6</td></tr>
<tr><td>5</td></tr>
</table>

Fonte: O autor

LEGENDA

NÍVEIS DE CLARIDADE DA NOITE			
NÍVEL	DEFINIÇÃO	MILILUX	ESTADO
5	Muito sombria	Até 0,7	Céu coberto
4	Sombria	Até 2	Sem nuvens e sem lua ou quarto de lua com
3	Intermediária	Até 10	Sem nuvens e com quarto de lua ou meia
2	Clara	Até 40	Sem nuvens com meia lua ou com lua cheia e nuvens
1	Muito Clara	Até 1000	Lua cheia sem nuvens

relativas a essas ações, o nível de claridade da noite e equipamentos optrônicos e ARP indicados para essas missões.

REFERÊNCIAS

ADAMY, D. (2004). EW 102: A Second Course in Electronic Warfare (1ª ed.). Londres: Artech House, 2004.

ALMEIDA, F. N. Inteligência Geoespacial e o uso de VANT (ARPS) pela Polícia Federal. Trabalho de Conclusão de Curso apresentado à Academia Nacional de Polícia como exigência parcial para a obtenção do título de Especialista em Ciência Policial e Inteligência. Brasília, 2012.

BLYENBURGH, P. V. UAS: The Global Perspective with a Focus on Light UAS. In: Seminário Internacional de VANT 2010. Palestras. São José dos Campos/SP, 27-29 de outubro de 2010.

BRASIL. Exército. EB20-MC-10.205: Comando e Controle. 1. ed. Brasília, DF, 2015.

BRASIL. Exército. EB20-MF-10.107: Inteligência Militar Terrestre. 2. ed. Brasília, DF, 2015.

BRASIL. Exército. EB20-MC-10.207: Inteligência. 1. ed. Brasília, DF, 2015.

BRASIL. Exército. EB70-MC10.223: Operações. 5. ed. Brasília, DF, 2017.

BRASIL. Exército. EB70-MC-10.307: Planejamento e Emprego da Inteligência Militar. 1. ed. Brasília, DF, 2016.

BRASIL. Exército. EB20-MC-10.214: Vetores Aéreos da Força Terrestre. 2. ed. Brasília, DF, 2020.

BRASIL. CIGE. Apostila de Guerra Eletrônica de Não Comunicações. Brasília, DF, 2012.

CORADESQUE, FELIPE A. A., DIEDRICH, Tiago J., ROSO, Nelson A. e CASTRO, Ruy M. Aplicações do Imageamento Termal no Reconhecimento. Encontro de Usuários de

Sensoriamento Remoto Das Forças Armadas – SERFA 2014. São José dos Campos, SP, Brasil, 09 a 12 de dezembro de 2014, IEAv.

EUA. Department of the Army. FM 3-0. Operations. Fevereiro, 2008.

JULIBONI, Márcio. A invasão dos drones: um negócio de US$ 55 bilhões. Exame.com, São Paulo, 10 jan. 2012. Disponível em: <http://exame.abril.com.br/negocios/noticias/a-invasao-dos-drones-um-negocio-de-us-26-bilhoes >. Acesso em: 09 Nov. 2016.

LAZARO, Fábio. O SARP Como Fonte de Imagens em Apoio ao
Reconhecimento, Vigilância e Aquisição de Alvos. 1 ed. Brasília: A Lucerna, 2015. Ano 4. Nr 06. 41p.

OLIVEIRA, Flavio Araripe de. CTA e o Projeto VANT. In: 1° Seminário Internacional de Vant. São José dos Campos, 2005. Palestra proferida no Centro Tecnológico da Aeronáutica em 11 jun 2005.

PIKE, J. E. Night Vision Goggles (NVG). 27 de Abril de 2005. Acesso em 19 de julho de 2017, disponível em: <http://www.globalsecurity.org/military/systems/ground/nvg.htm>. Acesso em: 02 Nov. 2016.

SAYLER, Kelley. A word of proliferated drones: A Technogy Primer. Center for a New American Security. p. 9 Washington, DC: 2015. Disponível em: < http://www.cnas.org/world-of-proliferated-drones-technology-primer#.VgyD6_RPjEY >. Acesso em: 10 Nov. 2016.

ARTIGO CIENTÍFICO

ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

A EFICIÊNCIA DE DIFERENTES MODULAÇÕES EM QUADRATURA NO EMPREGO DAS COMUNICAÇÕES DIGITAIS: UMA ANÁLISE SOBRE AS MODULAÇÕES 16 E 64-QAM.

FRANCISCO JOSÉ KLAUTH BRACCINI
MÁRIO ANTÔNIO COSTA SOUZA

RESUMO: A utilização de diferentes tipos de modulações nos equipamentos rádio é intrínseca ao emprego das comunicações. Sua relevância pode parecer invisível aos olhos humanos, mas faz toda a diferença para o emprego das comunicações via rádio. Nesse contexto, dentre as diversas modulações, este artigo apresenta a comparação entre dois tipos de modulações digitais em quadratura bastante usuais: 16 e 64-QAM, as quais possuem características que levam em consideração a escolha entre cobertura e capacidade de transmissão de dados. Tais fatores são peças fundamentais para a definição do resultado final que a estação de transmissora deseja alcançar. Na análise realizada, observaram-se as características de cada modulação QAM, tais como a probabilidade de bit errado e o ganho mínimo para a decodificação do serviço de rádio digital. Diante dessa análise, verificaram-se aspectos positivos e negativos destas modulações, os quais devem ser considerados ao empregá-las, a fim de obter a confiabilidade necessária na transmissão.

Palavras Chaves: CONFIABILIDADE, DECODIFICAÇÃO, DIGITAL RADIO MONDIALE.

1. INTRODUÇÃO

A tecnologia Digital Radio Mondiale – DRM (Report ITU-R BS.2384-0), criada em 1998, é um padrão internacional de radiodifusão digital, que possui largo emprego nas bandas de Ondas Médias (MF) e Ondas Curtas (HF). Também pode ser empregada na banda de uso comercial da FM Estendida, FM até a banda III do VHF e Ondas Longas (LF), sendo esta última banda comumente empregada na radiodifusão europeia.

Esta tecnologia, permite a transmissão de áudio de qualidade, imagens, texto, texto avançado para a organização estruturada em links de informações (Journaline). O DRM possui algumas variações, a saber:

• Tecnologia DIVEEMO: Plataforma de transmissão de vídeos em pequena escala, por meio da tecnologia DRM. Tal tecnologia, está em fase de desenvolvimento pelo instituto alemão Fraunhofer IIS e normatização junto à União Internacional das Telecomunicações (UIT). Essa tecnologia permite a transmissão de vídeos ao vivo em HF por exemplo.

• Tecnologia NAVIDATA (Recommendation ITU-R M.2058-0): destinada à navegação marítima, permite a transmissão de mensagens diversas sobre condições meteorológicas, segurança da embarcação, busca e salvamento, etc., de forma criptografada. Essa tecnologia utiliza uma arquitetura de transmissão muito similar à da tecnologia DRM.

Essas três tecnologias possuem em comum um importante aspecto: a utilização da modulação de amplitude em quadratura, do inglês, Quadracture Amplitude Modulation (QAM), na qual permite a codificação e decodificação dos diversos serviços proporcionados pelas plataformas de rádio digital.

2. DESENVOLVIMENTO

Ao enunciar a plataforma DRM, observa-

se que é uma tecnologia com grandes capacidades e que, em seus 22 anos de existência, alcançou uma maturação bastante significativa, se comparada aos antigos e consagrados métodos de transmissão em AM e FM.

No entanto, neste interim, surge a seguinte questão: quais os desafios a serem vencidos pelo rádio digital, para que conquiste o mesmo grau de confiabilidade e segurança frente às antigas tecnologias de modulação analógicas? Uma dessas variáveis, foco deste artigo, é a utilização correta da modulação digital QAM.

2.1 HIPÓTESE

Com o advento do Rádio Digital, as capacidades desse importante meio de comunicação se ampliaram: transmissão de áudio de qualidade, imagens, textos, até documentos e vídeos. No entanto, um importante paradigma precisa ser resolvido pelos operadores e pessoas envolvidas no planejamento do emprego desta moderna tecnologia: a dicotomia entre a capacidade de transmissão, a qual é intrínseca ao tipo de modulação digital, e a área de cobertura desejada.

2.2 OBJETIVO GERAL

Este artigo, busca trazer a reflexão do leitor, quanto ao correto emprego da tecnologia de rádio digital, de forma ampla. Para alcançar esse objetivo, este artigo traz um estudo de caso, de forma a fazer com que o leitor reflita sobre o emprego de diversas outras modulações, tendo como base o estudo da modulação QAM.

Desta forma, com o alcance desse entendimento, o emprego dessa tecnologia pode ocorrer de forma mais eficiente nos diversos cenários a serem enfrentados por pessoas que trabalham com a tecnologia, bem como no fornecimento de um melhor serviço ao usuário final. Não se trata de uma fórmula pronta, mas sim de uma trilha que pode ser a solução de diversas situações de emprego do sistema de radiocomunicação digital.

2.3 OBJETIVOS ESPECÍFICOS

O objetivo deste artigo é apresentar a os aspectos positivos e negativos, comparando as modulações 16 e 64-QAM, no que tange os parâmetros de recebimento dos serviços de radiodifusão DRM, com foco no canal de serviço principal, do inglês, Main Service Channel (MSC), o qual carrega em si os dados referentes aos serviços existentes na transmissão, seja áudio, imagem, texto, etc. Este parâmetro é decisivo para a análise da dicotomia capacidade de transmissão e cobertura.

2.4 JUSTIFICATIVA

Com a deficiente consciência sobre o correto emprego do sistema de radiodifusão digital em nosso país, tendo em vista que no meio civil não há serviço regular existente para a população em geral, as radiocomunicações militares têm sido empregada gradualmente, exigindo que os elementos envolvidos no emprego das comunicações se ambientem cada vez mais com os aspectos referentes à essa recente tecnologia.

Dessa forma, este artigo traz uma análise pontual do padrão DRM, que já é utilizado em diversos países do mundo. Esse padrão, possui receptores que possuem a capacidade de apresentar as características necessárias para o entendimento da dicotomia analisada e assim poder apresentar os resultados, que são de suma importância para o bom emprego do rádio digital.

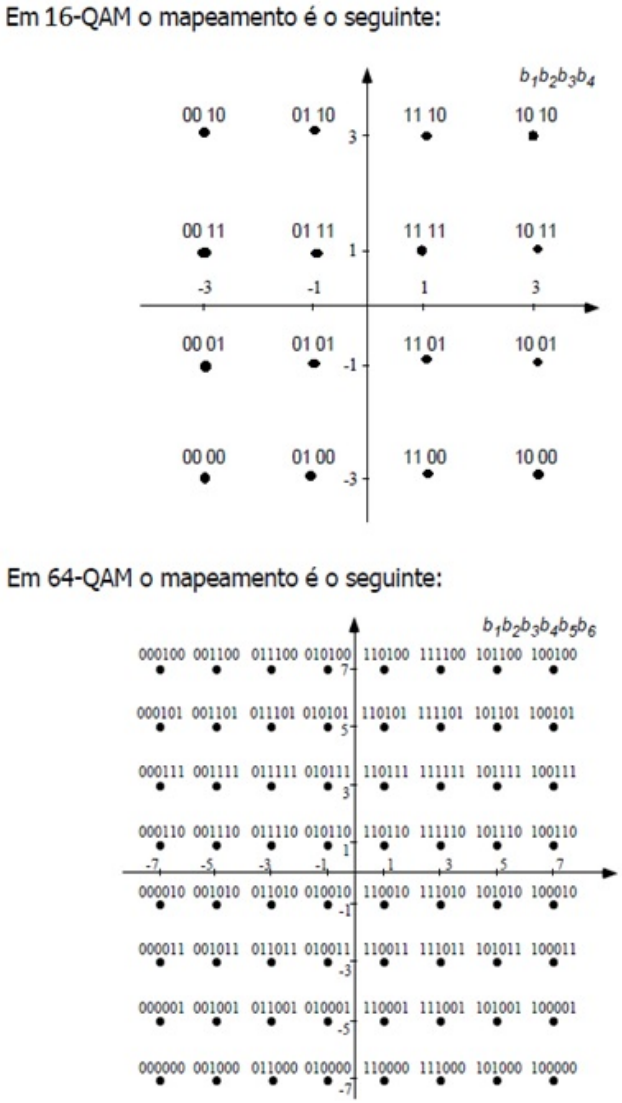
2.5 REFERENCIAL TEÓRICO

A linha de pesquisa adotada insere-se na linha de pesquisa bibliográfica, a qual está embasada nas obras de Fischer (2010), Laflin (2013), Spragg (2004), da Universidade de Porto (2019), bem como no tabelamento das características de recepção de estações DRM, com enfoque nos parâmetros de ganho mínimo e tipo de modulação.

2.6 METODOLOGIA

As modulações em QAM, são entendidas pelos equipamentos rádio através de uma série de cálculos realizados. Tais modulações se diferenciam pelos quantitativo de símbolos, o qual

FIGURA 1 Mapeamento ilustrativo das constelações de 16 e 64-QAM



Fonte: Universidade de Porto (2019), com edição do autor

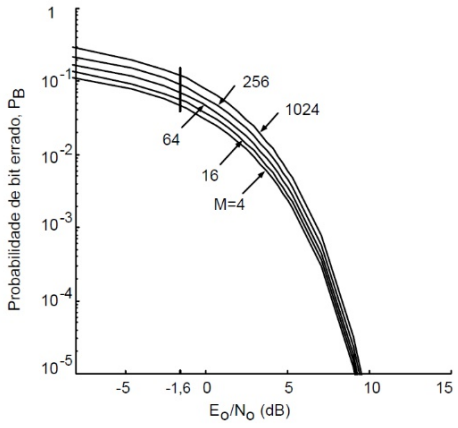
origina o tipo de modulação. Em 16-QAM há 16 símbolos representados, por exemplo. Na figura 1, as constelações de símbolos das duas modulações em análise são apresentadas pelo denominado diagrama de Gray, mapeados abaixo:

A fim de obter uma comparação adequada sob o ponto de vista prático, foram observadas as seguintes estações e seus parâmetros através do receptor DRM Uniwave Diwave 100, no período de janeiro a maio de 2020:

EMISSORA DRM	FREQUÊNCIA (KHz)	HORÁRIO DE BRASÍLIA	TAXA DE TRANSMISSÃO (Kbps)	MODULAÇÃO DO MSC (QAM)	POTÊNCIA (kW)	GANHO MÍNIMO PARA DECIDIFICAÇÃO
Rádio Romênia Internacional	9620	18:00	11,64	16	90	10 dB
Rádio Nacional da China	9655	7:30	14,56	16	30	10 dB
Rádio Martí (EUA)	7345	22:30	9,1	16	5	10 dB
Rádio Romênia Internacional	7315	17:00	21,00	64	90	17 dB
All India Radio	7550	18:00	17,44	64	500	17 dB

Observe que independente dos demais parâmetros da transmissão, a modulação em 16-QAM possui um ganho mínimo para decodificar os serviços DRM de 10dB, enquanto em 64-QAM, esse ganho passa para 17dB, fazendo com que o ouvinte que queira escutar uma das estações em 64-QAM, precise estar mais próximo do parque de transmissões da mesma ou a necessidade de uma elevada potência de transmissão a partir da emissora, devendo contar ainda com os efeitos da propagação, que interferem no ganho do receptor. Em contrapartida,

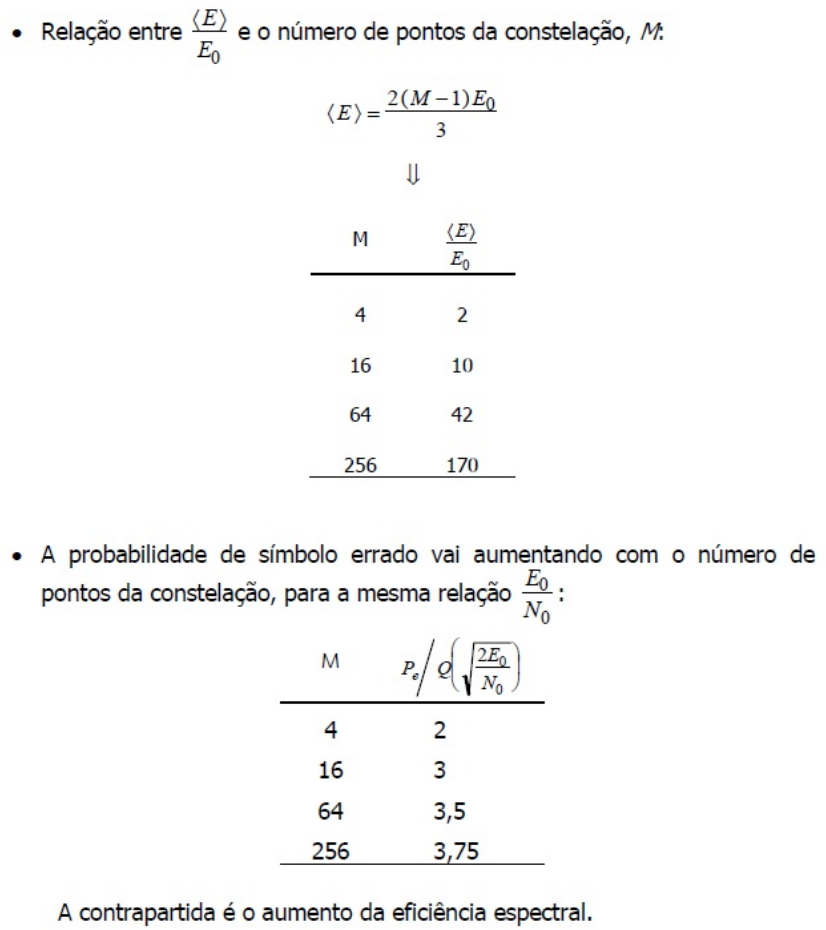
FIGURA 3 Gráfico da Probabilidade de bit errado



Fonte: Universidade de Porto (2019)

observa-se que a modulação de 64-QAM pode carregar até 21 kbps com a emissão da Rádio Romênia Internacional, proporcionando uma maior capacidade de transmissão de dados que a modulação 16-QAM, que se observou uma taxa máxima de 14,56 kbps, considerando-se que todas as estações transmitem com uma largura de banda de 10 kHz. Isso se explica na figura 1, pois quanto maior o número de símbolos, maior é a taxa de transmissão que uma determinada modulação pode carregar, ou seja, maior é a sua capacidade de transmissão.A limitação de

FIGURA 4 Probabilidade de bit errado



- Relação entre $\frac{\langle E \rangle}{E_0}$ e o número de pontos da constelação, M:

$$\langle E \rangle = \frac{2(M-1)E_0}{3}$$

$$\Downarrow$$

M	$\frac{\langle E \rangle}{E_0}$
4	2
16	10
64	42
256	170

- A probabilidade de símbolo errado vai aumentando com o número de pontos da constelação, para a mesma relação $\frac{E_0}{N_0}$:

M	$P_e \Big/ Q\left(\sqrt{\frac{2E_0}{N_0}}\right)$
4	2
16	3
64	3,5
256	3,75

A contrapartida é o aumento da eficiência espectral.

Fonte: Universidade de Porto

cobertura observada na modulação 64-QAM, pode é evidenciada através do comparativo da probabilidade de bit errado, nos diferentes tipos de modulação em QAM.

A probabilidade de bit errado se refere a eventuais erros que podem ocorrer na transmissão devido a diversos fatores, tais como, sinal fraco, interferências e a propagação.

Tendo como referência a figura 3, contendo o gráfico da probabilidade de erro, observe o demonstrativo matemático base do gráfico, que contém as modulações de 4, 16, 64 e 256-QAM:

Nota-se que a modulação 64-QAM possui uma probabilidade de erro de modulação maior que em 16-QAM, o que pode ser crucial para a transmissão da mensagem, que pode sofrer perdas por diferentes motivos no estabelecimento do enlace, resulta no comprometimento da eficácia e confiabilidade, tendo em vista a característica das emissões digitais necessitarem de um ganho mínimo para que

seus diversos serviços possam ser decodificados dentro de uma relação de erro de modulação aceitável ao receptor.

3. CONCLUSÕES

Conclui-se que a modulação 64-QAM possui uma maior capacidade de transmissão de dados, enquanto a transmissão em 16-QAM uma maior robustez às diversas interferências e perdas oriundas da realização de um enlace rádio.

Essa conclusão pode ser espelhada para os diversos tipos de modulação digitais existentes, ao se realizar um estudo de caso sobre qual modulação optar empregar. Um exemplo disso, se encontra nos transceptores militares Harris MPR-9600 Falcon II, que utilizam o modo de fonia MELP 600 e MELP 2400. Não coincidentemente, essa mesma lógica é vista, uma vez que a modulação MELP 600 possui menor taxa de transmissão e menor qualidade de áudio, no entanto alcaça maiores áreas de cobertura. Já a MELP 2400 possui maior qualidade de áudio, no entanto a possui um alcance, utilizando a potência no transceptor.

Por fim, espera-se que o leitor possa ter captado esse importante insigt, que é fundamental para o emprego do rádio, na Era das Comunicações Digitais, as quais fornecem serviços de qualidade, mas exigem cuidados em seu uso para sua boa utilização.

REFERÊNCIAS

FISCHER, Walter. Digital Video and Audio Broadcasting Technology. Londres: Springer, 2010.

ITU. Report ITU-R BS.2384-0: Implementation considerations for the introduction and transitionto digital terrestrial sound and multimedia broadcasting. Disponível em: < https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-BS.2384-2015-PDF-E.pdf>. 2015. Acesso em: 10 maio 2020.

ITU. Recommendation ITU-R M.2058-0: Characteristics of a digital system, named navigational data for broadcasting maritime safety and security related information from shore-to-ship in the maritime HF frequency band. Disponível em: < https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2058-0-201402-I!!PDF-E.pdf>. 2014. Acesso em: 10 maio 2020.

LAFLIN, Nigel. DRM Handbook. Geneva: DRM Consortium, 2019. Disponível em: < https://www.drm.org/wp-content/uploads/2019/02/DRM-Handbook.pdf>. Acesso em: 07 maio 2020.

SPRAGG, C. Donald. DRM Transmitter Requirements and Applying DRM Modulation to Existing Transmitters. Dallas: Continental Electronics Corp, 2004.

UNIVERSIDADE DO PORTO. Modulações digitais 5 “Quadrature Amplitude Modulation” (QAM) Detecção coerente e probabilidade de erro. Disponível em: < https://paginas.fe.up.pt/~sam/Tele2/apontamentos/Modul_QAM.pdf>. 2008. Acesso em 15 maio 2020.

ARTIGO CIENTÍFICO

ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

DESIGN DE ANTENA LOOP FRACTAL COM O SOFTWARE 4NEC2

CAP RAFAEL COSTA BARROS
ST WAGNER LEONARDO BELCHIOR E DUTRA

RESUMO :Este artigo apresenta um estudo com a finalidade de modelar uma antena do tipo loop fractal através do software de design de antenas “4NEC2”. Este trabalho buscou projetar uma antena com um comprimento reduzido, através da técnica de miniaturização, que fosse ressonante em 12 MHz. Inicialmente, empregou-se a geometria do tipo large loop devido a sua eficiência de radiação. Ao construir esse loop utilizou-se a geometria loop fractal do tipo “Koch Snowflake”, que garantiu um aumento do comprimento da antena, mas com uma área limitada.

Palavras Chaves: LOOP FRACTAL. MINIATURIZAÇÃO. 4NEC2.

1 INTRODUÇÃO

Atualmente, há uma tendência de que os componentes eletrônicos tornem-se cada vez menores e mais compactos. Isso possibilita seu emprego em uma gama maior de áreas, tanto civis quanto militares.

As antenas tipo “loop” apresentam simplicidade, baixo custo e versatilidade. Elas podem ter vários formatos: circular, triangular, quadrado, elíptico, etc. São amplamente utilizadas em links de comunicações até as bandas de microondas (até ± 3 GHz).

Neste artigo, uma antena foi proposta para possível emprego em um sistema de comunicações que necessite de antenas miniaturizadas. Uma das principais técnicas empregadas foi o uso de antenas com a geometria do tipo “loop fractal”, por permitir um aumento do comprimento da antena, sem aumentar a sua área. Uma grande parte dos estudos nos últimos anos empregou essa técnica para o design de antenas em UHF e SHF, para emprego em diversas aplicações como GPS, WiMax, radares e satélites.

2 DESENVOLVIMENTO

2.1 PROBLEMA

Como realizar a modelagem de antenas miniaturizadas para um sistema de comunicações, sem gastos com softwares pagos?

2.2 HIPÓTESE

Há uma grande quantidade de softwares que permitem a modelagem de antenas, neste trabalho foi empregado o programa gratuito “4NEC2”, que fornece ferramentas essenciais para o desenvolvimento de um projeto de antena.

2.3 OBJETIVO GERAL

Realizar a modelagem de uma antena miniaturizada através de software livre.

2.4 OBJETIVOS ESPECÍFICOS

a) Estabelecer qual software livre deve ser empregado para a modelagem de uma antena miniaturizada;

b) Realizar a modelagem de uma antena miniaturizada através de software livre.

2.5 JUSTIFICATIVA

Nas últimas décadas, uma grande quantidade de estudos buscou explorar as possibilidades de miniaturização de antenas,

as quais podem ser empregadas em sistemas de comunicações instalados em espaços físicos limitados, como viaturas ou aeronaves, além da vasta gama de aparelhos de emprego civil que empregam redes móveis.

2.6 REFERENCIAL TEÓRICO

Ao propor o estudo de antenas do tipo loop, verificou-se, durante a pesquisa, que em relação ao comprimento de onda empregado, podem ser classificadas como small loop ou large loop. Essa classificação é fundamental, pois estabelece características próprias para cada tipo de loop em relação à eficiência de radiação e à distribuição de corrente ao longo do loop.

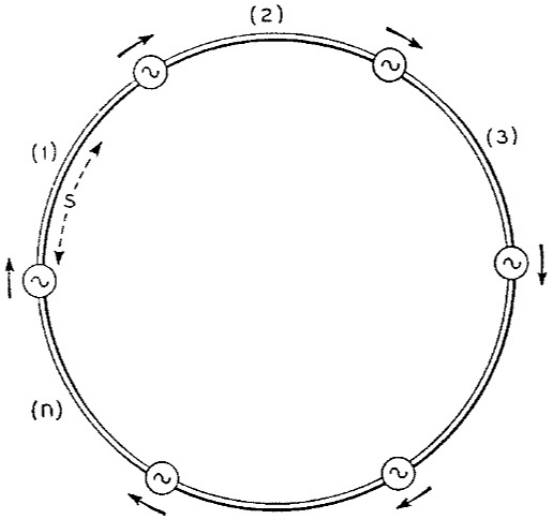
A modelagem da antena proposta neste artigo teve como principal objetivo miniaturizar o tamanho de uma antena com um padrão de radiação horizontalmente polarizado.

É importante saber que, no espaço livre, a antena loop com o maior ganho é a que abrange a maior área para uma dada circunferência, que é o loop circular, porém, é difícil de construir. A segunda melhor é a antena de loop quadrado (square loop), a qual pode ser alimentada para polarização horizontal ou vertical, simplesmente colocando o ponto de alimentação no centro de um braço horizontal ou no centro de um braço vertical.

Uma antena do tipo small loop possui o comprimento de até 0.1 (um décimo) do comprimento de onda (lambda), em que, considerando um square loop, cada lado é considerado um elemento de corrente uniforme modelado como um dipolo ideal. Enquanto uma antena do tipo large loop opera próxima ao primeiro ponto de ressonância, que ocorre a partir de 0.1 (um décimo) do comprimento de onda.

Ao analisar a distribuição de corrente em uma antena do tipo loop, conforme [1], [2] e [4], verifica-se que em antenas do tipo small loop há uma distribuição de corrente substancialmente uniforme, com amplitude e fase constantes, mas com uma resistência de radiação muito baixa e uma elevada reatância indutiva, que causa dificuldades para o casamento de impedância e dificuldades para o seu uso em aplicações que necessitem transmissão. No entanto, em antenas do tipo large loop verificamos uma resistência de radiação maior, mas com uma distribuição de corrente não uniforme ao longo do loop, com variação da amplitude e fase, a menos que seja estabelecida nesse large loop a impressão de fontes de corrente de maneira uniforme, conforme a figura 1.

FIGURA 1: Distribuição uniforme de fontes em uma antena Loop



Fonte: Neha, 2014.

O principal problema ao modelar uma antena nesse contexto, conforme [2], trata-se da forma como as fontes serão impressas ao longo do loop.

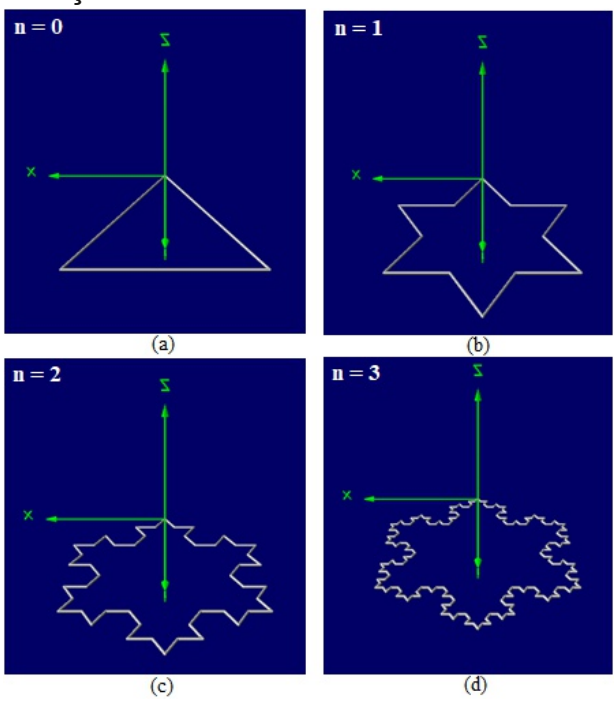
Buscou-se na pesquisa projetar uma antena a ser empregada para uma frequência de 12 Mhz, com uma necessidade específica de se ter o menor comprimento possível, mas com uma eficiência de radiação adequada para o emprego proposto.

O principal fator empregado para a miniaturização foi o uso da geometria fractal [6], [7], [8] e [9] do tipo Koch Snowflake. Essa geometria estabelece uma antena loop fractal com sua forma originada a partir de “iterações” (programação de repetição de uma ou mais ações), que são feitas em cada um dos lados de um triângulo equilátero inicial. Essa geometria tem como uma das principais vantagens o aumento regular do perímetro, mas com um aumento reduzido da

área ocupada pela antena. Dessa forma, consegue-se atingir o comprimento ótimo para ressonância da antena, mas com uma área reduzida.

Neste artigo, a antena projetada tem um comprimento ótimo para a frequência de operação de 12 MHz. A partir dessa frequência de operação, tem-se que o comprimento de onda (λ) nesse emprego é de 25 metros (m). Dessa forma, a modelagem da antena fractal deve ser construída com um comprimento aproximado de 01 (um) lambda, ou seja, 25 m. O comprimento da antena (C) foi obtido a partir do emprego do software 4nec2, que permite o cálculo da impedância da antena e o comprimento em que antena foi ressonante para a frequência de 12 MHz.

FIGURA 2: Iterações Koch Snowflake: (a) 0 iteração, (b) 1 iteração, (c) 2 iterações, (d) 3 iterações.



Fonte: Neha, 2014.

Neste estudo, foi feito o cálculo do tamanho do lado do triângulo equilátero inicial, que a partir das iterações permite o aumento do comprimento da antena, mas com um aumento da área reduzido. Os valores do lado inicial do triângulo; do perímetro inicial do triângulo; do perímetro final do fractal; da relação entre o comprimento da antena (C) e comprimento de onda (λ) e da impedância estão apresentados nas tabelas 1, 2 e 3. Foi empregado o software 4NEC2 para a modelagem da antena e para o cálculo da impedância.

TABELA 1: RELAÇÃO ENTRE O COMPRIMENTO DA ANTENA FRACTAL E A IMPEDÂNCIA PARA A ITERAÇÃO 1

Lado inicial (m)	Perímetro Inicial (m)	Perímetro Final (m)	C / λ	Impedância
5.6250	16.8750	22.50	0.90	62.8 – 567j
6.2500	18.7500	25.00	1.00	72.3 – 300j
6.8750	20.6250	27.50	1.10	92.1 – 65j
7.0000	21.0000	28.00	1.12	97.7 – 19j
7.0625	21.1875	28.25	1.13	101 + 4.87j
7.1250	21.3750	28.50	1.14	104 + 28.7j

TABELA 2: RELAÇÃO ENTRE O COMPRIMENTO DA ANTENA FRACTAL E A IMPEDÂNCIA PARA A ITERAÇÃO 2

Lado inicial (m)	Perímetro Inicial (m)	Perímetro Final (m)	C / λ	Impedância
4.6875	14.0625	25.00	1.00	47.3 – 555j
5.1563	15.4688	27.50	1.10	55.1 – 315j
5.6250	16.8750	30.00	1.20	70.0 – 98.1j
5.7188	17.1563	30.50	1.22	74.2 – 54.7j
5.8125	17.4375	31.00	1.24	78.8 – 10.5j
5.8594	17.5781	31.25	1.25	81.4 + 11.8j

TABELA 3: Relação Entre O Comprimento Da Antena Fractal E A Impedância Para A Iteração 3

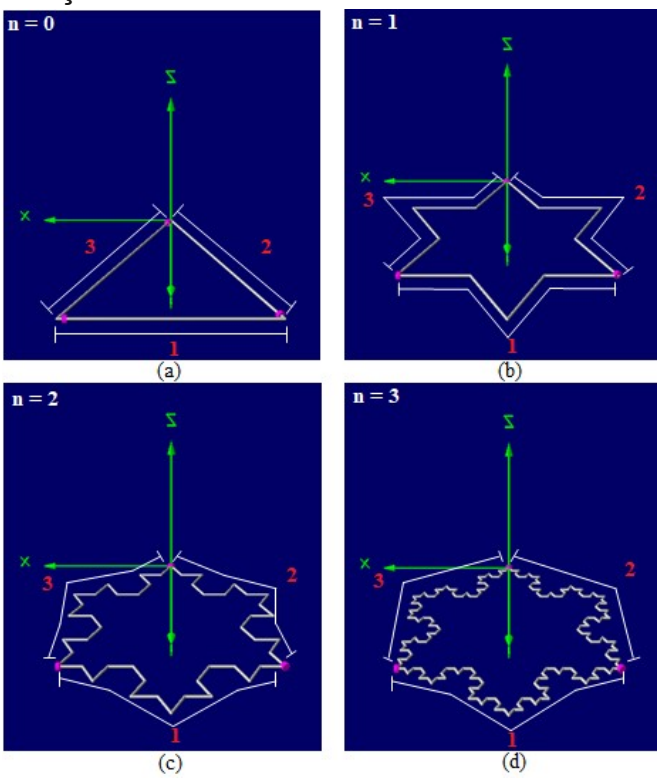
Lado inicial (m)	Perímetro Inicial (m)	Perímetro Final (m)	C / λ	Impedância
4.92	14.76	35	1.40	56.7 – 107j
4.99	14.98	35.5	1.42	60.0 – 70j
5.06	15.19	36	1.44	63.4 – 31j
5.10	15.29	36.25	1.45	65.5 – 8j
5.13	15.40	36.5	1.46	67.2 + 9j
5.20	15.60	37	1.48	71.4 + 49.6j

Nos resultados apresentados nas tabelas 1, 2 e 3, pode-se verificar que a ressonância ocorre para valores, da relação entre comprimento da antena e comprimento de onda, de 1.12, 1.24 e 1.45 respectivamente para as iterações 1, 2 e 3.

O tipo de antena modelado acima, com apenas uma fonte de energia, estabelece uma corrente que não é uniforme ao longo do loop, consequentemente, não garante um padrão de radiação constante. Uma solução proposta para o design da antena em questão permite, ao distribuir as fontes de corrente de maneira uniforme ao longo do loop, um padrão de radiação horizontalmente polarizado, considerando que o loop esteja no plano horizontal.

Ao empregar essa geometria, a antena proposta foi dividida em 03 (três) pétalas, em que uma pétala consiste em uma sequência de segmentos ligados, que são excitadas a partir da linha de alimentação localizada no primeiro segmento de cada pétala. Cada pétala é alimentada individualmente. Na figura 3 podemos verificar uma aplicação do loop fractal proposto por , em que são estabelecidas fontes de corrente em cada uma das três pétalas.

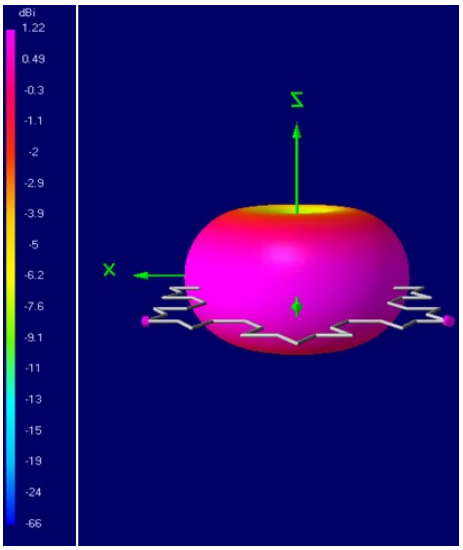
FIGURA 3: Iterações Koch Snowflake e a divisão da antena em 03 pétalas: (a) 0 iteração, (b) 1 iteração, (c) 2 iterações, (d) 3 iterações.



Fonte: Neha, 2014.

Na figura 4 podemos verificar o padrão de radiação, obtido a partir do 4NEC2, do Loop fractal com 03 (três) pétalas e 2 (duas) iterações. Um padrão de radiação horizontalmente polarizado conforme proposto no trabalho.

FIGURA 04 : Padrão de Radiação do Loop fractal com 03 pétalas e 2 iterações.



Fonte: Neha, 2014.

3. CONCLUSÃO

Neste trabalho, foi estabelecido um projeto para miniaturização de uma antena ressonante para a frequência de 12 MHz através do desenvolvimento de uma antena loop Fractal. Inicialmente, empregou-se uma antena do Tipo Large Loop, que permite uma adequada resistência de radiação. Empregou-se ainda a geometria fractal do tipo snowflake, pois possibilita um aumento do comprimento da antena, mas com um limitado aumento de área da mesma e, ainda, mantém o formato de loop. Em seguida, realizou-se a divisão do loop em três partes, com a finalidade de se ter uma corrente uniforme, que possibilitou uma antena com um padrão de radiação horizontalmente polarizado.

REFERÊNCIAS

Warren L. Stutzman, Gary A. Thiele. Antenna Theory and Design. John Wiley & Sons, 2012.

Sergei A. Schelkunoff e Harald T. Friis. Antennas: theory and practice. New York: Wiley; London: Chapman & Hall, 1952.

Andrew Alford e A. G. Kandoian. Ultrahigh-Frequency Loop Antennas. AIEE Transactions, 1940.

C.-C. Lin, L.-C. Kuo, e H.-R. Chuang. A Horizontally Polarized Omnidirectional Printed Antenna for WLAN Applications. IEEE Transactions on Antennas and Propagation, Vol. 54, No. 11, November 2006.

O. F. G. Palacios, R. E. D. Vargas, J. A.Heraud. Perez e S. B. C. Erazo. S-Band Koch Snowflake Fractal Antenna for Cubesats. IEEE, 2016.

S. Neha A., P. C. Dalsania e H. J. Kathiriya. Analysis of Koch Snowflake Fractal Antenna for Multiband Application. International Journal of Engineering Research & Technology (IJERT), 2014.

N. S. Dandgavhal e M. B. Kadu. Design and Simulation of Koch Snowflake Fractal Antenna for GPS, WiMAX and Radar Application. IEEE Bombay Section Symposium (IBSS), 2015.

R. Hasse, V. Demir, W. Hunsicker, D. Kajfez, e A. Elsherbeni. Design and Analysis of Partitioned Square Loop Antennas. ACES Journal, Vol. 23, Nº. 1, March 2008.

D. H. Werner e S. Ganguly. An Overview of Fractal Antenna Engineering Research. IEEE Antennas and Propagation Magazine, Vol.45, Nº1, 2003.

ARTIGO CIENTÍFICO

ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

O USO DA FERRAMENTA GNS3 PARA CONSTRUÇÃO DE UM AMBIENTE VIRTUALIZADO PARA CURSOS DE CIBERNÉTICA.

1° SGT MNT COM TIAGO WASEM ZIEMBOWICZ
2° SGT MNT COM MAURO DIEGO ANDRADES DEGLIOMENI

RESUMO:Este artigo descreve o uso da ferramenta GNS3 para construção de um ambiente virtualizado para cursos de cibernética. A pesquisa foi conduzida em áreas relacionadas à prática de laboratórios virtuais em cibernética, para suporte ao ensino-aprendizado. Com base nisso, foram estudadas algumas ferramentas para construção de ambientes virtuais e escolhido o GNS3 (Graphical Network Simulator-3) para essa finalidade. Posteriormente, foi projetada uma arquitetura de rede, similar a um SOC (Security Operations Center) com diversos ativos de rede e máquinas virtuais. Esses últimos, com a finalidade de prover serviços de rede, segurança e monitoramento, foram implementados no GNS3. Após a configuração da arquitetura de rede, testes foram realizados e os resultados apresentados demonstraram a eficiência da ferramenta ao emular a arquitetura de rede proposta. Desta maneira, o ambiente virtualizado proporciona aos alunos mais oportunidade de executarem atividades práticas em cibernética, além do aumento de habilidades e conhecimentos na área.

Palavras Chaves: VIRTUALIZAÇÃO, GNS3, CIBERNÉTICA, LABORATÓRIO.

1 INTRODUÇÃO

Inúmeras são, atualmente, as ameaças à segurança das redes ao redor do mundo. Destacam-se os códigos maliciosos, comumente chamados de malware. O relatório do diretor executivo de segurança da informação da empresa de tecnologia CISCO aborda, em uma de suas seções, a preocupação com a evolução do malware (CISCO, CISO Benchmark, 2019).

Os malwares podem ter diversos objetivos, estando entre os principais a forma de expansão das “botnets”, redes de computadores infectadas utilizadas para fins maliciosos [CISCO, Relatório de Ameaças, 2019]. O combate às botnets se dá por meios de ativos de segurança de redes, como firewalls e sistemas de detecção e prevenção de intrusão, do inglês, Intrusion Detection System (IDS) e, Intrusion Prevent System (IPS).

O desenvolvimento de mecanismos para detecção constitui-se em uma atividade complexa e trabalhosa, que envolve pesquisa e experimentação. Assim, trabalhos que buscam este desenvolvimento, contribuem verdadeiramente para a evolução tecnológica dos ativos de segurança de redes, bem como para a manutenção da segurança no espaço cibernético (GÓMES CARMONA, 2017).

No entanto, implementar ativos e ferramentas para realizar o monitoramento e prevenção das ameaças cibernéticas, requer elevado investimento financeiro, conforme aponta o relatório de Cybersegurança de 2020 da empresa multinacional de tecnologia da informação Accenture.

Adquirir hardwares específicos para equipar laboratórios com o objetivo de treinamento e ensino na área de cibernética, tornou-se cada vez mais oneroso. Além da possibilidade desses hardwares tornarem-se obsoletos em um curto espaço de tempo, é necessário adquirir uma quantidade considerável de equipamentos para equipar um laboratório que atendesse satisfatoriamente a um mínimo de 10 alunos. Sendo assim, um recurso menos dispendioso, que serve ao propósito do ensino e treinamento em cursos ou estágios de cibernética, é a virtualização.

A virtualização já está bastante

consolidada em ambientes de servidores e datacenters (VMWARE, 2020). Quanto ao uso desse mecanismo em ambientes de ensino-aprendizagem na área de cibernética, é o que se pretende discutir neste trabalho.

O intuito da pesquisa será explorar a ferramenta GNS3 (Graphical Network Simulator-3), um software livre que tem por finalidade emular ambientes complexos de rede, disponibilizando ao usuário uma quantidade considerável de ativos para pesquisa e experimentação (GNS3, 2020). Neste contexto, o estudo irá concentrar-se no uso do GNS3 para emular cenários voltados ao ensino em cursos e estágios de proteção cibernética.

2 DESENVOLVIMENTO

Um dos aspectos da proteção cibernética é a segurança de uma rede, usada para garantir a conexão entre inúmeros dispositivos. Desse modo, especialistas em segurança devem, constantemente, passar por treinamentos nos vários aspectos de segurança da rede, ter uma forte base de conhecimento dos diversos serviços de rede e como podem ser protegidos frente às ameaças, na proporção que elas apareçam (CHAPMAN, 2017).

Realizar o treinamento desses especialistas, para que possam responder com eficiência às ameaças em uma rede, requer um ambiente sofisticado, atualizado e dinâmico. Posto isso, a pesquisa irá abordar o uso da virtualização dos serviços de rede, analisando as principais ferramentas destinadas a essa finalidade, suas características e demonstrar o motivo da escolha do software GNS3 para esse trabalho.

Os emuladores de rede oferecem a possibilidade de imitar uma rede sem a necessidade de alguns componentes, como cabos para conexão de dados e rede elétrica. (LANDERS, 2019). A seguir, serão apresentadas as principais ferramentas que podem emular topologias de redes, tanto de baixa como alta complexidade.

2.1 VIRTUALIZADORES DE REDE

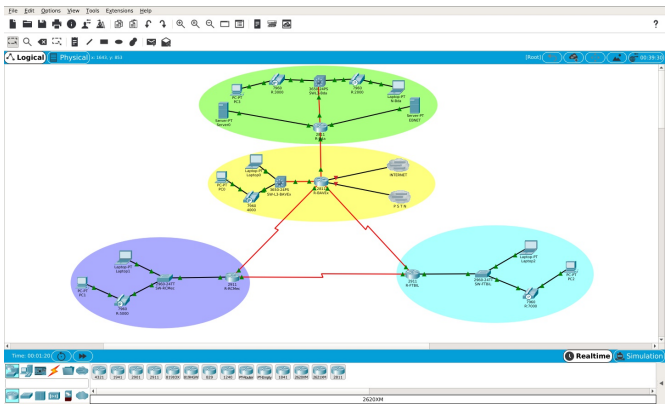
2.1.1 CISCO PACKET TRACER

O packet tracer foi desenvolvido para o ensino de redes de computadores com simulações baseadas nos níveis de conhecimento exigido para obter uma certificação cisco CCNA ou CCNP. É um programa gratuito, com interface gráfica simples e amigável, proporcionando a simulação de ativos de rede, principalmente switches e roteadores da Cisco (PACKET TRACER, 2020).

O programa pode ser utilizado em sistema operacional Windows e Linux. A versão 7.2.1 do Packet Tracer contém recursos para simular soluções de Internet das Coisas (IoT), projetos inteligentes, como cidades e casas inteligentes, com a possibilidade de utilizar Python e Java Script para programar seu comportamento (PACKET TRACER, 2020).

No entanto, o packet tracer não possibilita a integração com uma variedade de dispositivos intermediários ou finais, como soluções de firewall open source e desktop Linux. Está limitado a dispositivos da própria CISCO. A figura 1 mostra um exemplo de uma topologia de rede na interface do packet tracer 7.2.1 para Linux.

FIGURA 1: Topologia de Rede



Fonte: o autor

2.1.2 EVE-NG

O EVE-NG (Emulated Virtual Environment – Next Generation) é uma ferramenta para emulação de ambientes de

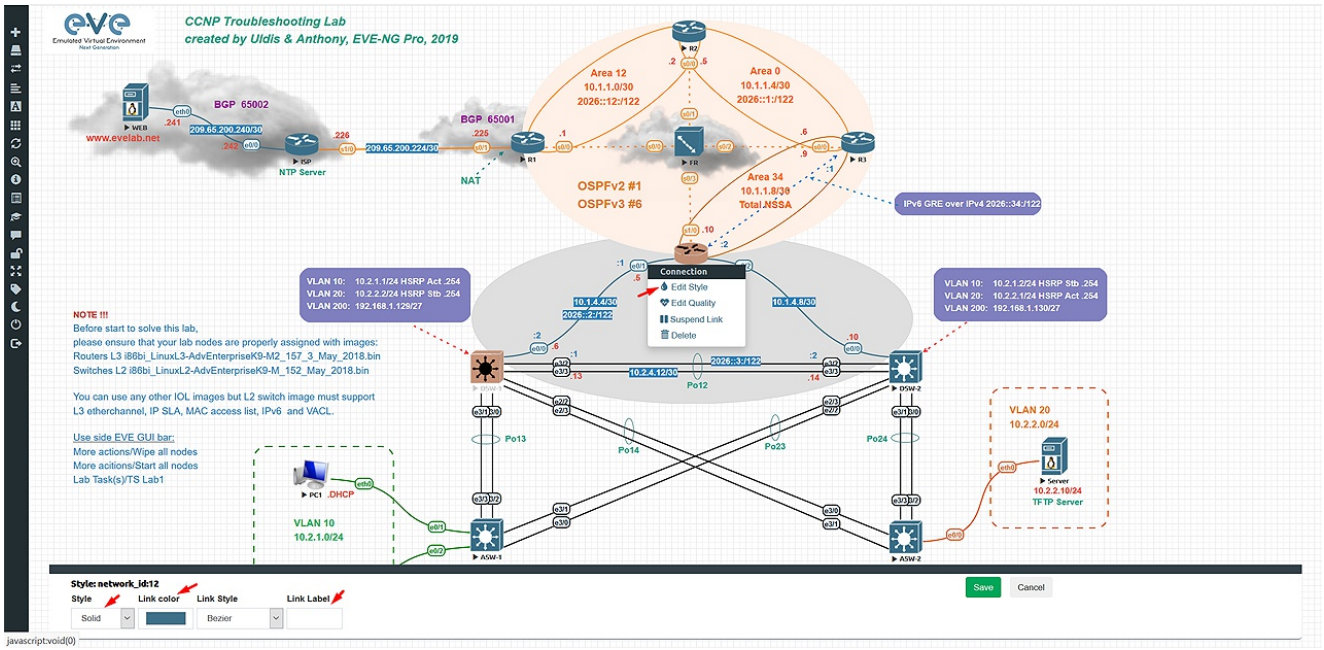
rede que vem sendo bastante aplicada em testes de vulnerabilidades de segurança, para testar novas tecnologias como as Redes Definidas por Software (SDN – Software Defined Network) ou para desenvolvedores que desejam testar seus softwares (BALYK, 2019).

Com o EVE, pode-se emular redes corporativas complexas, homologar soluções e mudanças em uma topologia antes de colocá-las em produção. Outros recursos interessantes são a construção de ambientes de POCs (Proof of Concepts) para clientes, a análise de tráfego de pacotes com o programa Wireshark e testes em soluções para problemas reais (BALYK, 2019).

Este emulador está disponível nas versões Community Edition, Professional Edition e Learning Centre Edition. A versão Community é gratuita, oferecendo menos recursos que a versão profissional, que é paga, mas, mesmo assim, a versão gratuita possibilita a criação de inúmeros cenários de rede. Deve ser instalado preferencialmente em ambiente de servidor, pois requer recursos de hardware consideráveis para um correto desempenho (EVE-NG, 2020).

Uma das vantagens do EVE-NG é a possibilidade de integração com vários tipos de dispositivos de diversos fabricantes, como Cisco, Checkpoint, Palo Alto, PfSense, Mikrotik, Dell, HP, entre outros. Através da integração com o emulador “Dynamips”, pode emular o hardware de switchs e roteadores da Cisco, e com o software livre QEMU, possibilita a execução da maioria dos sistemas operacionais como Linux, Windows, FreeBSD e outras arquiteturas suportadas (BALYK, 2019). A figura 2 exibe um exemplo de topologia de rede elaborada no EVE-NG.

FIGURA 2: Topologia de rede EVE



Fonte: www.eve-ng.net

2.1.3 GNS3

O GNS3, do inglês “Graphical Network Simulator-3” é um emulador de software de rede que permite a combinação de dispositivos virtuais e reais, usados para simular redes complexas (GNS3, 2020).

É uma ferramenta de código aberto e utiliza vários softwares emuladores como o Dynamips, Dynagen, QEMU, Docker, VirtualBox, entre outros, capazes de emular ambientes baseados em Linux e Windows, além dos diversos dispositivos de rede dos principais fabricantes do mercado (WONLY;SZOLTYSIK, 2014).

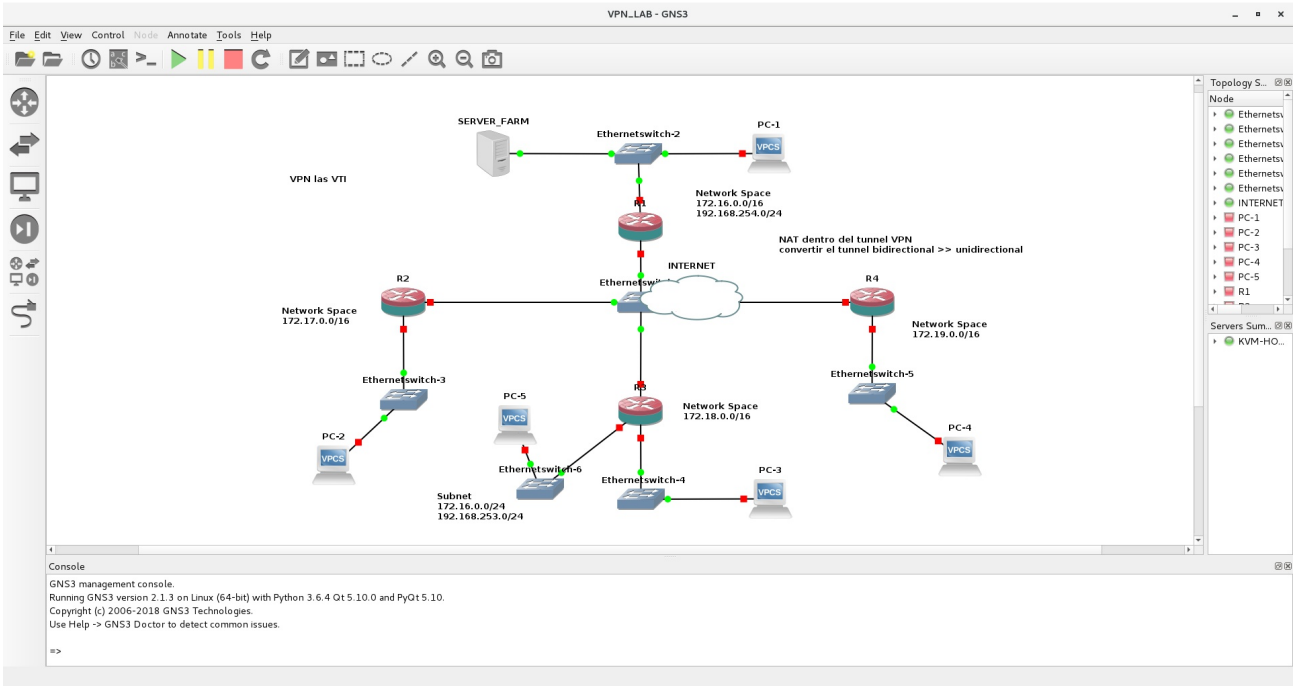
O GNS3 pode ser instalado nas plataformas Linux, Windows e MAC OS, oferecendo também um conjunto de funcionalidades ao se integrar com aplicativos terminais como Putty, VNC, Gnome Terminal,

Windows telnet client, entre outros. Realiza integração também com o Wireshark, fazendo captura e análise de pacotes, assim como em um ambiente de rede virtual (MOHTASIN, 2016).

Uma das vantagens do GNS3 é a simulação de rede em tempo real para testes de pré-implementação, sem a necessidade de hardware de rede e a criação de mapas de rede dinâmicos para a solução de problemas e teste de prova de conceito (GÓMEZ CARMONA, 2017).

A seguir, a figura 3 mostra um exemplo da interface GUI do GNS3.

FIGURA 3: Interface do GNS3



Fonte: https://gns3.com

A tabela a seguir resume as principais características e recursos das três ferramentas para virtualização de redes encontradas na homepage de cada uma delas:

TABELA1: Comparação entre virtualizadores de rede

Característica / Recurso	Ferramentas		
	Packet Tracer	EVE-NG Community	GNS3
Versão Atual	7.2.1	2.0.3-110	2.2.8
Tipo	simulador	emulador	emulador
Licença	livre	livre	livre
Custos	gratuito	gratuito	gratuito
Instalação	fácil	complexa	complexa
Processador	n/a	Core i5	Core i5
Memória	n/a	8 GB	*gb
HD	n/a	50 GB	35 GB
Virtualização	não	sim	sim
Integração	apenas cisco	vários	vários

Fonte: autores

Importante destacar que os dados compilados na tabela se referem aos requisitos mínimos para instalação. O número de instâncias virtuais que podem ser implementadas varia com a capacidade do hardware físico no qual está instalada a ferramenta.

2.2 MODELO PROPOSTO

Após uma breve análise das ferramentas, levando principalmente em consideração o objetivo da pesquisa, sobre um ambiente virtual adequado para o ensino de proteção cibernética, optou-se pela ferramenta GNS3. A principal vantagem apresentada pelo GNS3 frente as outras ferramentas, foi o fato de ser totalmente gratuito e possibilitar uma integração com um número considerável de sistemas operacionais e dispositivos de rede.

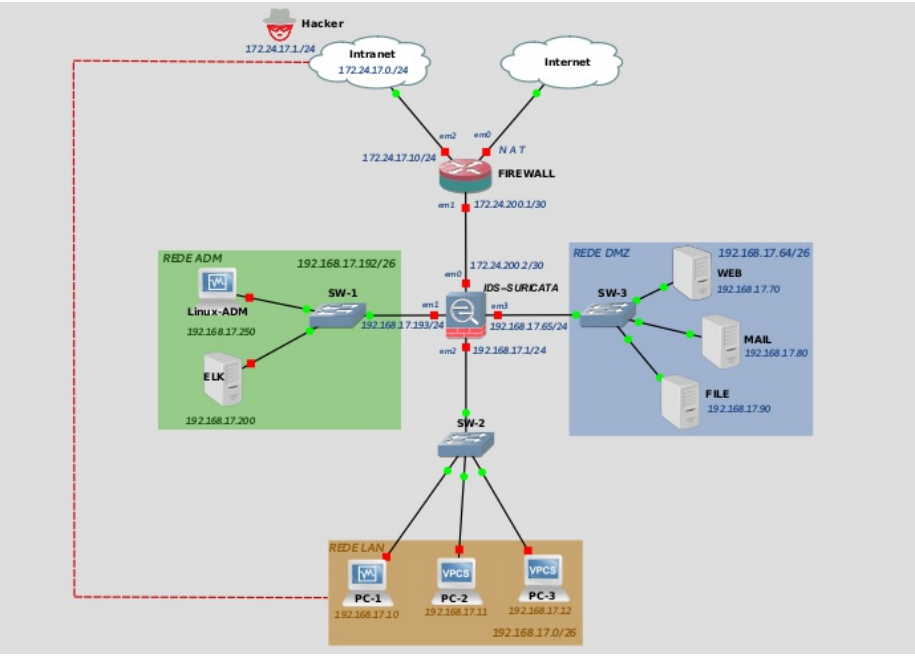
O packet tracer fica limitado apenas aos dispositivos de rede da cisco e estes não possuem os mesmos recursos disponíveis nos equipamentos reais. O EVE-NG, apesar de ser uma ferramenta excelente para o acesso remoto, em sua versão gratuita, não é integrado dinamicamente com o wireshark, recurso importante para análise de pacotes e essencial em assuntos que envolvem proteção cibernética.

Vários outros quesitos que serão tratados nas próximas seções deste artigo favoreceram a utilização do GNS3.

Diversos cenários poderiam ser implementados na abordagem de uma topologia de rede voltada à proteção cibernética. Dessa forma, a topologia proposta visa apresentar uma rede de baixa complexidade, porém voltada a explorar os serviços de rede mais visados por cibercriminosos, bem como as ferramentas necessárias para identificar e tentar reduzir possíveis ataques.

A figura 4 apresenta a topologia de rede que será trabalhada nessa pesquisa, os serviços de rede implementados e os recursos necessários para realizar a proteção da rede, ambiente totalmente virtualizado, gerenciado pelo GNS3.

FIGURA 4: Topologia GNS3



Fonte: autor

2.2.1 TOPOLOGIA DE REDE

Para cumprir o objetivo de apresentar um ambiente virtual capaz de simular uma rede voltada à proteção cibernética, resolveu-se utilizar os dispositivos de rede descritos a seguir, que representam a arquitetura mínima em um Centro Operacional de Segurança, (SOC - Security Operational Center) (DEMERTZIS, 2019):

2.2.1.1 FERRAMENTAS DE SEGURANÇA E MONITORAMENTO:

Firewall: o sistema escolhido foi o pfSense, que é uma distribuição de firewall de rede gratuita, baseada no sistema operacional FreeBSD com um kernel personalizado e incluindo pacotes de software livre de terceiros para funcionalidades adicionais (PFSENSE, 2020).

IPS/IDS: O Suricata é um mecanismo de detecção de ameaças à rede gratuito e aberto, maduro, rápido e robusto. O mecanismo Suricata é capaz de detecção de intrusão em tempo real (IDS), prevenção de intrusão em linha (IPS), monitoramento de segurança de rede (NSM) e processamento de pcap (captura de pacotes) offline. O pacote Suricata foi instalado no sistema pfSense. (SURICATA, 2020).

Servidor ELK-Stack: "ELK" é o acrônimo para três projetos open source: Elasticsearch, Logstash e Kibana. O Elasticsearch é um mecanismo de busca e análise. O Logstash é um pipeline de processamento de dados do lado do servidor que faz a ingestão de dados a partir de inúmeras fontes simultaneamente, transforma-os e envia-os para um “esconderijo” como o Elasticsearch. O Kibana permite que os usuários visualizem dados com diagramas e gráficos no Elasticsearch. A pilha ELK foi instalada em uma VM (Virtual Machine) com sistema operacional Debian9. (ELK, 2020)

2.2.1.2 SERVIÇOS DE REDE

Servidor WEB: uma VM com sistema operacional Debian 9 e com o servidor web Apache2 instalado.

Servidor MAIL: uma VM com sistema operacional Debian 9 simulando um servidor de e-mail.

Servidor FILE: uma VM com sistema operacional Debian 9 simulando um servidor de FTP.

2.2.1.3 DEMAIS ATIVOS

PC ADM: uma VM com sistema operacional Debian9 e GUI XFCE, com a finalidade de realizar a gerência dessa arquitetura.

PC1, PC2 e PC3: Vms com sistema operacional Debian 9 e GUI XFCE que representam a rede LAN nessa topologia, ou seja, o usuário final.

A topologia é completada com três switchs e duas nuvens NAT (Network Adress Translation), onde uma simula uma rede intranet e outra a internet. Todas as máquinas virtuais mencionadas são integradas ao GNS3 através do VirtualBox. O ícone representando um Hacker é uma VM com o Sistema Operacional Kali Linux, também integrado por meio do VirtualBox.

A versão do GNS3 na qual foram realizados os testes é a 2.2.5 para Linux, pois a ferramenta está instalada em um notebook com sistema operacional Debian GNU/Linux 9 (stretch) 64-bit, com 16 GB de memória RAM, processador Intel Core i5-4200U CPU de 1.60GHz × 4 (quad-core) e disco de 240 GB HD SSD. A versão do VirtualBox utilizada nos testes é a 6.0.4 para o Linux Debian.

3 CONCLUSÃO

3.1 TOPOLOGIA E CONECTIVIDADE

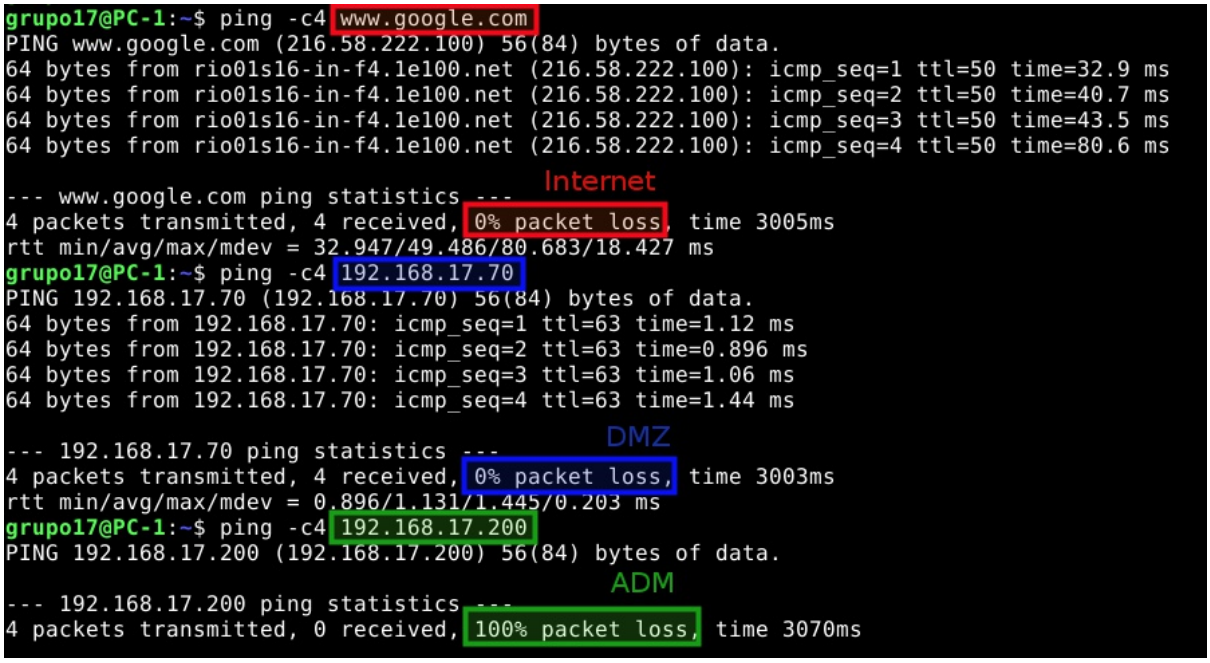
Com a finalidade de validar a topologia apresentada na seção anterior, interconectar e integrar seus elementos, foram realizados testes de conectividade entre os dispositivos.

3.1.1 CONECTIVIDADE COM A REDE LAN

A figura 5, demonstra que tomando como origem o PC-1, utilizando o comando ping obtivemos sucesso na comunicação da rede LAN com as redes externas conectadas e ele,

quais sejam, Internet e rede DMZ. A rede LAN não tem acesso para a rede ADM.

Figura 5: Conectividade com a LAN

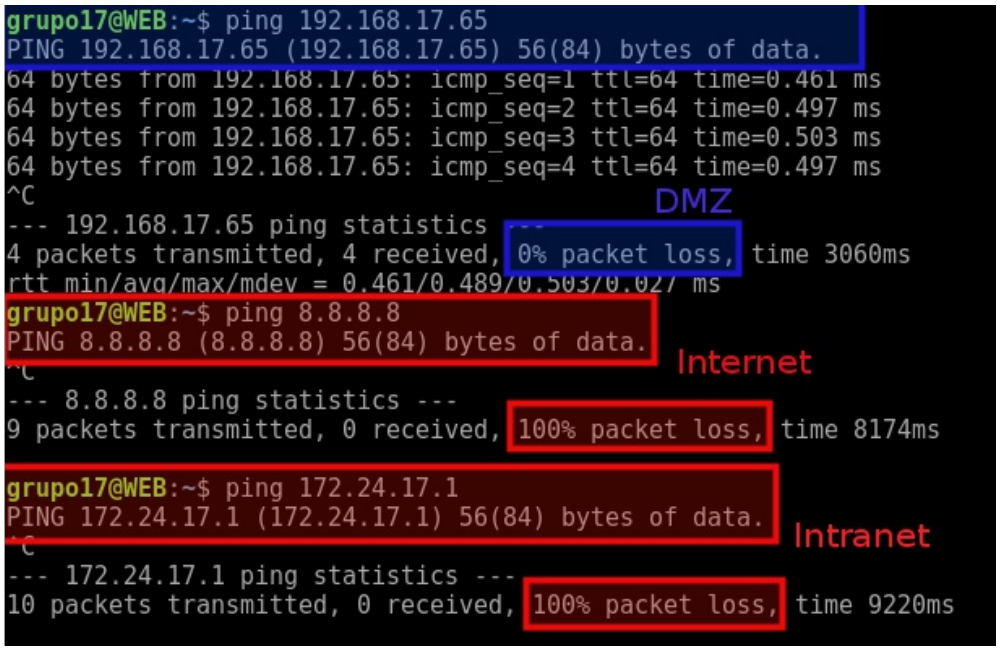


Fonte: autores.

3.1.2 CONECTIVIDADE DA REDE DMZ

A Figura 6, demonstra que utilizando como origem o Servidor WEB, obtivemos sucesso na comunicação dentro da própria DMZ, mas a mesma não se comunica com as redes intranet e internet, devido às configurações realizadas no firewall. Não foram permitidos que pacotes icmp originados da rede DMZ saíssem para a internet ou intranet, comportamento esse, padrão para uma rede DMZ.

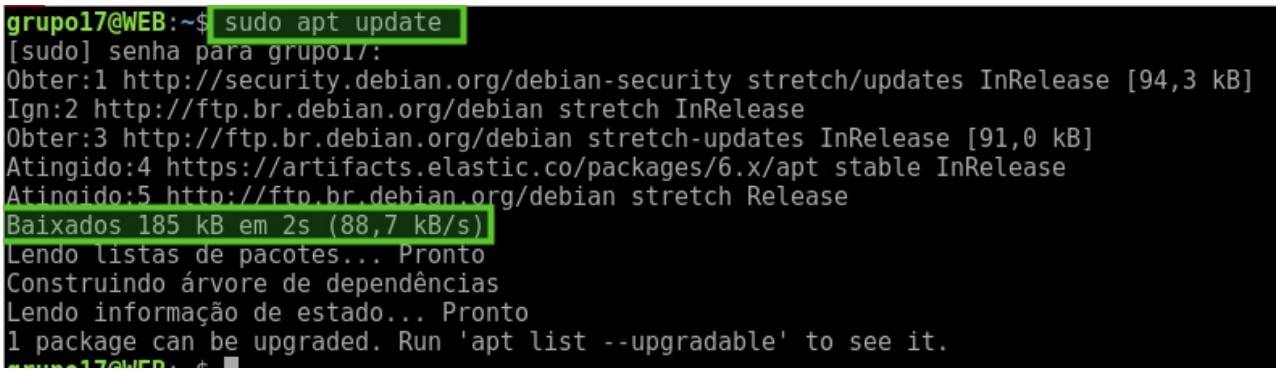
FIGURA 6: Conectividade com a DMZ



Fonte: autor.

Para comprovar que a configuração do firewall só bloqueou a saída de pacotes icmp para internet oriundos da DMZ, a figura 7 exibe o resultado de uma atualização de pacotes (comando update) realizado através do servidor WEB.

FIGURA 7: Atualização de pacotes

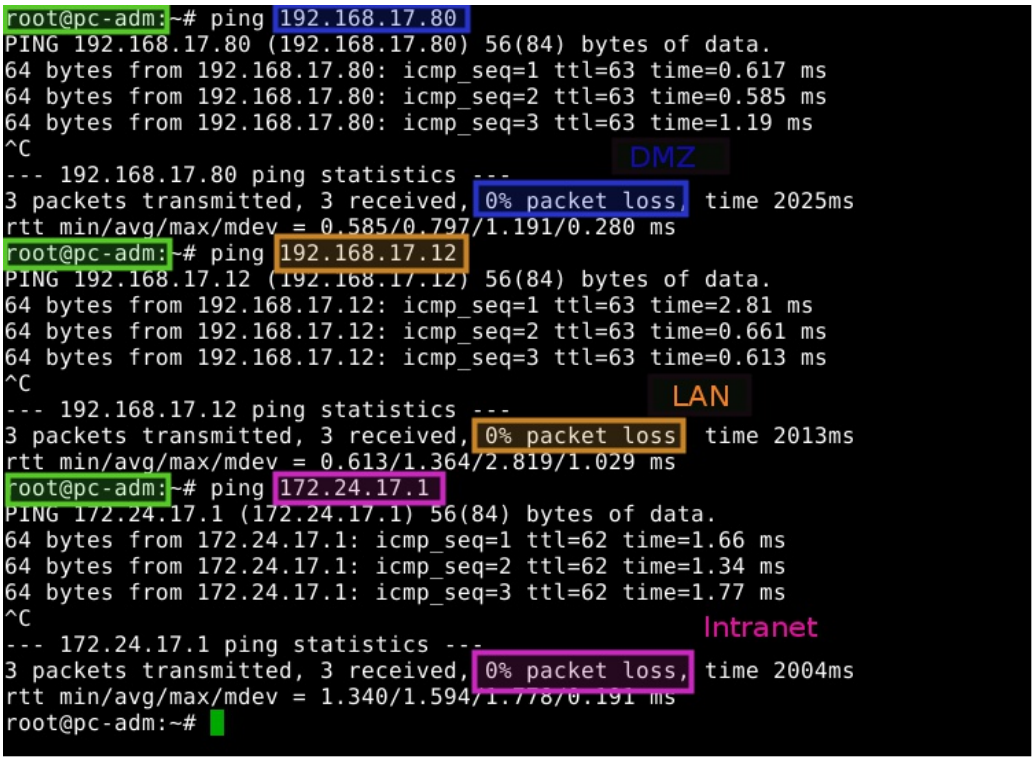


Fonte: autor.

3.1.3 CONECTIVIDADE DA REDE ADM

A figura 8, exibe a comunicação originando do PC-ADM para a rede DMZ, LAN e Intranet, através do comando ping. O host PC-ADM deve ter conectividade com todas as redes pois é o host responsável pela gerência da rede.

FIGURA 8: Conectitidade com a rede ADM



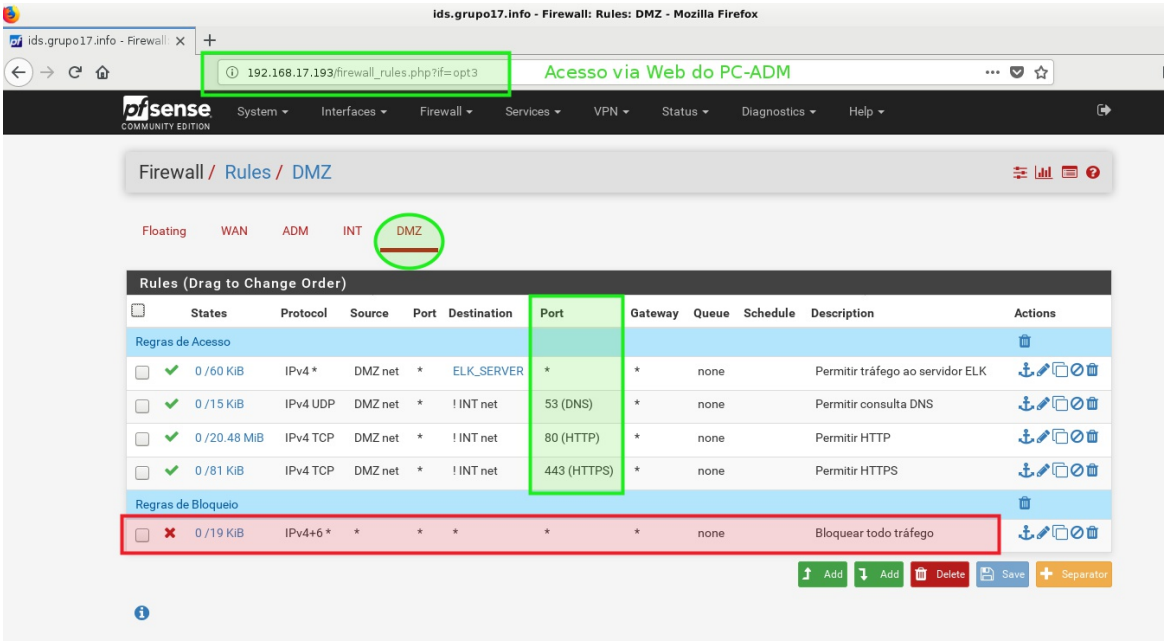
Fonte: autor.

Os testes de conectividade demostraram que o GNS3 consegue realizar a gerência das interfaces de rede das Vms do VirtualBox, o que comprova a integração bem sucedida entre as ferramentas.

3.2 REGRAS DE FIREWALL

Os resultados obtidos nos testes de conectividade apresentados na subseção anterior, principalmente aqueles referentes à rede DMZ com saída para internet e intranet, foram fruto das configurações realizadas no firewall. As regras de firewall da rede DMZ estão descritas na figura 9.

FIGURA 9: Regras de Firewall



Fonte: autor.

Através da imagem, verificamos que as regras foram configuradas no firewall pfSense em sua interface web via PC-ADM. Essa configuração comprova que a topologia de rede no GNS3 se comporta como se fosse uma arquitetura real. O usuário ou aluno que utiliza esses recursos dificilmente observará alguma diferença, proporcionando assim, habilidades práticas elevadas que auxiliam consideravelmente na construção do seu conhecimento.

3.3 GERAÇÃO DE TRÁFEGO TCP

Com a finalidade de realizar mais testes no ambiente virtual, esta subseção está dedicada à geração de tráfego TCP. A geração desse tráfego possibilita testar a integração do GNS3 com o aplicativo de captura de tráfego wireshark (WIRESHARK, 2020), com o auxílio do programa “Iperf”, que tem por finalidade testar a largura de banda em uma conexão, utilizando protocolos como TCP, UDP, FTP e outros (IPERF, 2020).

As figuras 10 e 11, mostram respectivamente a geração do tráfego TCP via iperf de um host cliente (Kali Linux), situado na rede intranet para o servidor WEB hospedado na DMZ.

FIGURA 10: Tráfego TCP cliente

```
root@twz-debian:/home/tiagowz# iperf -c 192.168.17.70
------------------------------------------------------------
Client connecting to 192.168.17.70, TCP port 5001
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 172.24.17.1 port 48944 connected with 192.168.17.70 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  84.2 MBytes  70.3 Mbits/sec
```

Fonte: autor.

FIGURA 11: Tráfego TCP servidor

```
grupo17@WEB:~$ iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
[  4] local 192.168.17.70 port 5001 connected with 172.24.17.1 port 48944
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.1 sec  84.2 MBytes  69.8 Mbits/sec
```

Fonte: autores.

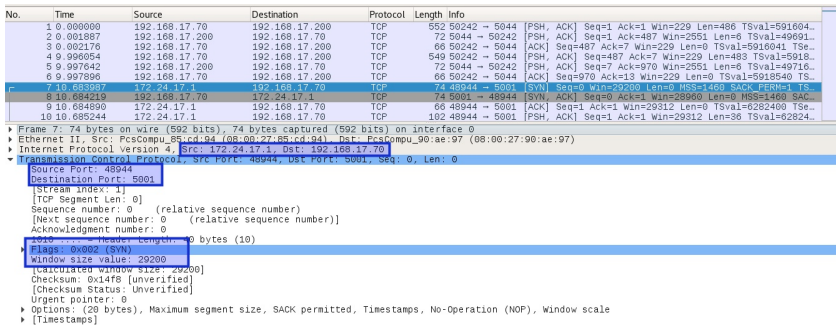
Importante destacar que, antes de se iniciar o programa iperf, foi realizada a captura de tráfego via wireshark no GNS3, na conexão entre o servidor Web e o switch 3. O tráfego foi originado da Intranet (HostOnly) no VirtualBox, por isso o endereço que origina a conexão analisada por meio do wireshark é o endereço IP do firewall (172.24.17.1:48944) gateway da rede intranet. O destino da conexão é o host WEB (192.168.17.70:5001). Nesse host, o Iperf está rodando em modo servidor. Na análise do tráfego TCP, figura 12, podemos observar o seguinte:

Antes do início da comunicação entre o cliente na Intranet e o Servidor WEB, acontece o processo de handshake TCP. O cliente envia o pacote SYN (pacote de sincronismo que é o primeiro passo para iniciar qualquer conexão numa rede TCP/IP) ao servidor, esse responde ao cliente com um pacote SYN/ACK. O processo de handshake do TCP termina quando o cliente envia o pacote ACK confirmando ao servidor que recebeu o SYN/ACK e a comunicação pode começar.

A comunicação do cliente é realizada na porta 48944 e o servidor recebe a conexão na porta TCP padrão que o Iperf trabalha, a porta 5001.

Ao final do fluxo de TCP entre cliente e servidor (quando o Iperf termina o fluxo) as mensagens trocadas entre servidor e cliente são o [FIN,ACK], onde o servidor informa que não tem mais nada a transmitir e o cliente responde ao servidor com o [ACK] e depois envia um [FIN,ACK] ao servidor que responde a finaliza a comunicação com um [ACK].

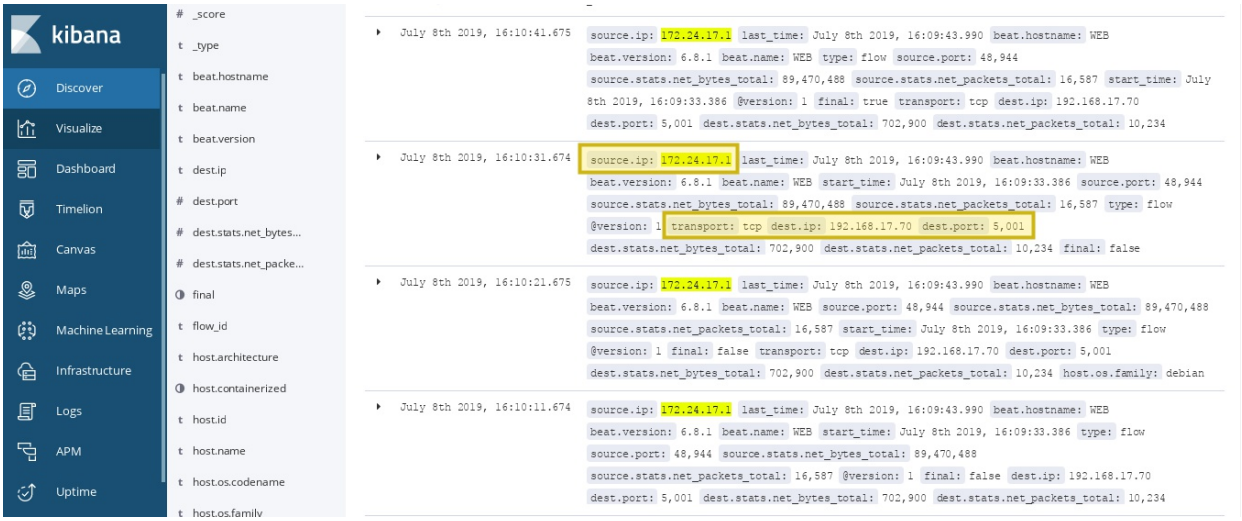
FIGURA 12: Captura wireshark



Fonte: autor

Para finalizar os testes desta seção, serão apresentados os logs do tráfego TCP gerado via iperf. Os logs são exibidos do servidor ELK da rede ADM, conforme representados na figura 13:

FIGURA 13: Visualização de logs no Kibana



Fonte: autor.

Ao implementar uma busca simples, com o endereço IP da Intranet (172.24.17.1), observamos que os logs do tráfego gerados via Iperf foram enviados com sucesso. Nesse log, identifica-se o endereço IP de origem (172.24.17.1), porta de origem (48944), endereço IP de destino (192.168.17.70), porta de destino (5001) e o tipo de protocolo da camada de transporte (TCP). Ao verificar que os logs estão sendo gerados, certifica-se que a infraestrutura de rede montada está funcional, e o servidor ELK funcionando de forma correta para analisar os logs do tráfego gerados para teste.

3.4 AVALIAÇÃO

Os resultados apresentados nessa seção puderam mostrar a eficiência do GNS3 quanto à criação de um laboratório virtual para trabalhar em cursos de cibernética. Vale destacar a importância da integração com o VirtualBox, tornando o laboratório muito flexível com a execução de inúmeras tarefas de rede, idênticas ao mundo real. O ambiente do laboratório é um bom campo de testes para estudantes em cibernética antes de começar trabalhando com equipamentos reais, onde erros podem causar falhas catastróficas (MOHTASIN, 2016).

Vale destacar que o laboratório virtual é ideal para alunos que tentam aprender como instalar, configurar e testar os dispositivos de rede, bem como arquiteturas e topologias de rede voltadas à proteção cibernética. Não é adequado para testar o desempenho dos dispositivos de rede, pois o resultado não pode ser comparado com um ambiente real.

O número de instâncias virtuais que são adicionadas em um laboratório é limitado à capacidade do hardware físico subjacente. Para criar um laboratório com mais recursos, ativos de rede e máquinas virtuais, precisa-se de mais capacidade de hardware na máquina física.

O ambiente virtual proposto é usado em máquina local, apesar do GNS3 permitir a execução de laboratórios de forma remota, o estudo foca na criação de laboratório local hospedado em sistema operacional Linux. A vantagem de usar o GNS3 em SO Linux é a

possibilidade de utilizar a integração de recursos como Docker, máquinas virtuais QEMU, sem a necessidade de uma máquina virtual GNS3, conhecida como GNS3 VM, necessária quando instalado em sistema operacional Windows. O próprio kernel do Linux se encarrega de disponibilizar esses recursos, economizando recursos de hardware do hospedeiro (GNS3, 2020).

Assim, se implementado com sucesso, este laboratório pode ser usado como recurso essencial para que os alunos realizem práticas de rede e cibernética. Além disso, o ambiente do laboratório é totalmente escalável, podendo ser replicado e implementado em outro computador. Os alunos devem ser capazes de implementar facilmente instâncias de dispositivos de rede da vida real, fornecendo uma maneira acessível e de baixo custo para executarem práticas de rede e cibernética.

3.5 CONSIDERAÇÕES FINAIS

O principal objetivo deste artigo foi apresentar a ferramenta GNS3 como solução para elaboração de ambientes virtuais para a prática de atividades em cursos de proteção cibernética. Criar um laboratório virtual, ajuda a superar os problemas existentes de hardware e acessibilidades limitadas. O ambiente apresentado permite configurar, gerenciar e testar diversos dispositivos de rede e máquinas virtuais, proporcionando a aquisição de habilidades práticas aos alunos.

No campo da cibernética integram-se diferentes tipos de hardware, software e ambientes de telecomunicações. Existe uma quantidade significativa de conhecimento e desenvolvimento de habilidades necessárias para trabalhar na área cibernética. De acordo com Tegliacane et al (2016), no geral, os alunos precisam de oportunidades em alternadas soluções de laboratório para que possam desenvolver os conhecimentos necessários. Desta maneira, poderão construir e manter sistemas computadorizados e em rede, mesmo quando o acesso ao treinamento físico do hardware é limitado.

Além disso, uma pesquisa realizada em 2019 mostrou que alunos com oportunidade de realizarem atividades práticas (laboratórios) na área de TI tem desempenho superior na aquisição de habilidades em comparação àqueles que possuem apenas hardwares físicos (limitados a execução de testes) para executarem exercícios práticos (LANDERS, 2019).

À vista disso, os simuladores de habilidades em tecnologia da informação (TI) podem ser usados para complementar ou substituir hardware caro para o ensino e aprendizagem em computadores e habilidades de software, redes e segurança cibernética (DEWEY & SHAFFER, 2016; GERCEK, SALEEM, & STEEL, 2016). Segundo Ghani (2015), os avanços tecnológicos tornaram possível que objetivos previamente alcançados apenas com a realização de atividades práticas, hoje pudessem ser atingidos usando simulações.

Nesse sentido, este artigo propôs o uso do GNS3 como ambiente virtual para prática de atividades nos cursos de cibernética, proporcionando aos alunos, criarem, testarem e analisarem seus próprios laboratórios em um ambiente praticamente livre de custos.

REFERÊNCIAS

BALYK, Nadiia et al. Designing of Virtual Cloud Labs for the Learning Cisco CyberSecurity Operations Course. 2019.

CHAPMAN, Samuel et al. Can a network attack be simulated in an emulated environment for network security training?. Journal of Sensor and Actuator Networks, v. 6, n. 3, p. 16, 2017.

DEMERTZIS, Konstantinos et al. A próxima geração do centro de operações de segurança cognitiva: arquitetura lambda analítica adaptativa para defesa eficiente contra-ataques adversários. Big Data e computação cognitiva , v. 3, n. 1, p. 6, 2019.

GHANI, Usman. Efeito de mecanismos de feedback no aprendizado dos alunos no uso de treinamento baseado em simulação em um

programa de engenharia da computação. In: Conferência de Líderes de Engenharia 2014 sobre Educação em Engenharia. Imprensa da Universidade Hamad bin Khalifa (HBKU Press), 2015. p. 59

GÓMEZ CARMONA, Joaquín. Proposta de manual de práticas de laboratório de redes usando o emulador GNS3. 2017. Tese de Doutorado. Universidade Central "Marta Abreu" de Las Villas, Faculdade de Engenharia Elétrica, Departamento de Eletrônica e Telecomunicações.

LANDERS, Kathy Michelle. Usando simulações para se preparar para faculdades e carreiras em tecnologia da informação. 2019.

MOHTASIN, R. et al. Desenvolvimento de um laboratório de rede virtualizado usando as estações de trabalho GNS3 e VMware. In: Conferência Internacional de 2016 sobre comunicações sem fio, processamento de sinais e redes (WiSPNET) . IEEE, 2016. p. 603-609.

SILVA, Isaias Batista da et al. Gnsmood: um aplicativo web integrado ao ambiente virtual de aprendizado que permite a comunicação de dispositivos de rede com o servidor de simulação gns3. 2018.

WOLNY, Wiesław; SZOŁTYSIK, Mateusz. Visão geral da virtualização de ambientes de redes de computadores existentes para aprendizado de redes de computadores. Studia Ekonomiczne , v. 188, p. 250-264, 2014.

ACCENTURE, Ratório de Cybersegurança 2020. Disponível em https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf. Acesso realizado em 08 de maio de 2020.

CISCO, Cybersecurity Series 2019 - CISO Benchmark. Disponível em:< https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/ciso-benchmark-optimized.pdf?.>. Acesso em: 28 abr de 2020.

CISCO, Cybersecurity Series 2019 - Threat. Disponível em: <https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/cybersecurityseries-threat.pdf?.> Acesso em: 28 abr de 2020.

ELK, 2020. Disponível em:< https://www.elastic.co/pt/what-is/elk-stack.> Acesso em: 14 de abr de 2020.

EVE-NG, 2020. Disponível em https://www.eve-ng.net/index.php/documentation/. Acesso realizao em 26 de abril de 2020.

GNS3, Software, 2020. Disponível em https://gns3.com/software. Acesso realizado em 24 de abril de 2020.

IPERF, 2020. Disponível em https://iperf.fr/. Acesso realizado em 07 de maio de 2020.

PACKET TRACER, 2020. Disponívelm em https://www.netacad.com/pt-br/courses/packet-tracer. Acesso realizado em 26 de abril de 2020.

PFSENSE, 2020. Disponível em https://www.pfsense.org/. Acesso realizado em 14 de abril de 2020.

VMWARE, Virtualização, 2020. Disponível em https://www.vmware.com/br/solutions/virtualization.html. Acesso realizado em 24 de abril de 2020.

WIRESHARK, 2020. Disponível em https://www.wireshark.org/. Acesso realizado em 02 de maio de 2020.

ARTIGO CIENTÍFICO

ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

ENERGIA SOLAR FOTOVOLTAICA: SOLUÇÃO PARA PELOTÕES ESPECIAIS DE FRONTEIRA ENQUANTO COMUNIDADES ISOLADAS

1º TEN ANDRÉ RICARDO SILVA VIEIRA DOS SANTOS
2º SGT ADRIANO RIBEIRO PACHECO

RESUMO: A Amazônia Legal tem sido foco de diversas ameaças, tais como, narcotráfico, imigração ilegal, tráfico de armas, garimpo ilegal, biopirataria e extração ilegal de madeira. E nesse sentido, a presença do Exército Brasileiro se torna de extrema importância à manutenção da soberania nacional. Destaca-se o emprego das diversas unidades de fronteira no combate aos delitos transfronteiriços e ambientais. São os denominados Pelotões Especiais de Fronteira (PEF), elementos avançados, que marcam a presença do Exército Brasileiro e do Estado na região. Com foco na segurança nacional, o Exército Brasileiro tem investido em recursos humanos e, principalmente, em tecnologia, por meio dos projetos estratégicos. Mas, ainda perduram as dificuldades encontradas na maioria dos PEF, o que não é diferente dos núcleos habitacionais que crescem em torno deles. Sabe-se que um dos fatores limitadores do poder operativo do PEF é a questão da energia elétrica, que é provida apenas por algumas horas do dia e através um gerador a diesel. Através deste artigo, baseado em pesquisa bibliográfica, de artigos, livros periódicos e em legislações nacionais, é possível apresentar a geração de energia solar fotovoltaica dentre os meios energéticos sustentáveis, visando reduzir o uso de combustível fóssil e a proporcionar o uso de uma energia limpa e segura para os PEF enquanto comunidades isoladas, suprindo assim as dificuldades logísticas encontradas em manter o gerador a diesel.

Palavras Chaves: AMAZÔNIA LEGAL; EXÉRCITO BRASILEIRO; ENERGIA SOLAR; PELOTÕES ESPECIAIS DE FRONTEIRA.

1 INTRODUÇÃO

Áreas como a Amazônia Legal, que apresentam tesouros minerais e biológicos de valor incalculável, têm sido foco de diversas ameaças, tais como: narcotráfico, tráfico de armas, garimpo ilegal, biopirataria e extração ilegal de madeira. Nesses locais, a presença do Exército Brasileiro é de vital importância para a manutenção da soberania nacional.

Os Pelotões Especiais de Fronteira do Exército Brasileiro (PEF) são estabelecidos como primeira linha de vigilância em regiões inóspitas da Amazônia e, apesar da sua importância, ainda encontram grandes dificuldades quanto à geração de energia elétrica, um fator limitador do poder operativo destes Pelotões. Os PEF, estando nas condições de comunidades isoladas, suprem a falta da rede convencional de energia elétrica empregando geradores a diesel, que além do impacto negativo ao meio ambiente, tem seu uso racionado para economia de combustível, justificado pelo regrado apoio logístico de suprimento, manutenção e transporte.

Baseado em pesquisa bibliográfica, o presente artigo trata da importância do emprego do sistema de energia solar fotovoltaica, como possível solução para suprir a deficiência energética nos Pelotões Especiais de Fronteira do Exército Brasileiro, enquanto comunidades isoladas.

2 DESENVOLVIMENTO

2.1 AMAZÔNIA LEGAL E O EXÉRCITO BRASILEIRO NA FAIXA DE FRONTEIRA

A Amazônia é o maior bioma do Brasil e um dos mais ricos em biodiversidade do mundo. Embora a maior parte de sua extensão esteja inserida no território brasileiro, a floresta amazônica, como também é conhecida, se estende por mais oito países. Segundo Lima (2018):

“O Bioma Amazônia é um conjunto de

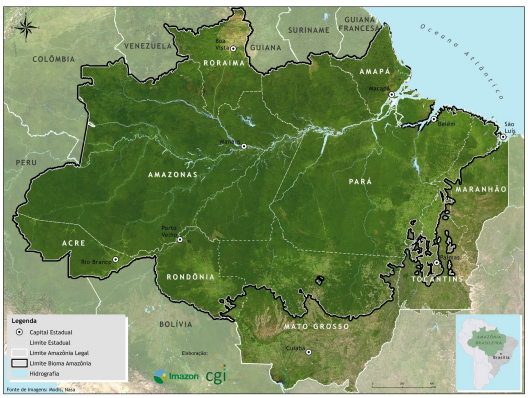
ecossistemas interligados pela Floresta Amazônica e pela Bacia Hidrográfica do Rio Amazonas, a mais densa de todo o planeta. Caracteriza-se pela sua elevada extensão, ocupando quase a metade do território do Brasil, além das áreas territoriais da Bolívia, Guiana, Guiana Francesa, Suriname, Peru, Colômbia, Venezuela e Equador. “

Outro conceito merece destaque, o da Amazônia Legal. Criada pela Constituição de 1946, regulamentada pela Lei nº 1.806, de 6 de janeiro de 1953, e conforme aponta Menin (2007, p. 41):

“é fruto de um conceito político e não de um imperativo geográfico, com vistas à necessidade do Governo de planejar o desenvolvimento da região, é constituída pelos territórios dos Estados do Pará, Amazonas, parte do Maranhão, Mato Grosso e Tocantins, e dos antigos territórios, hoje Estados do Amapá, Roraima, Acre e Rondônia”

Como se pode observar na Figura 1:

FIGURA 1 : Amazônia Legal



Fonte: NASA.

A Amazônia Legal tem sido foco de diversas ameaças, como narcotráfico, imigração ilegal, tráfico de armas, garimpo ilegal, biopirataria e extração ilegal de madeira. É nesse sentido que a presença do Exército Brasileiro se torna de extrema importância à manutenção da soberania nacional, e conforme pontuado por Lima (2018):

“...é um grande desafio manter a faixa de fronteira, especificamente da Amazônia, livre das atuais ameaças que assolam a região. A Amazônia Brasileira é um patrimônio fabuloso [...]. Os olhos do mundo estão voltados para ela, pelo imenso potencial ali presente [...]. O momento atual traz consigo oportunidades e desafios: desenvolver, de forma sustentável, sem maniqueísmos, esta vasta região; garantir a presença soberana do Estado Brasileiro em uma área sujeita à cobiça internacional; melhorar as condições de vida da nossa população ali instalada, levando-lhe alternativas econômicas viáveis, serviços públicos de qualidade e preservar a riquíssima cultura local.”

Com foco na segurança nacional, o Exército Brasileiro tem investido em recursos humanos e, principalmente, em tecnologia, por meio de projetos estratégicos, tendo como exemplo, o Sistema Integrado de Monitoramento de Fronteiras – SISFRON, de forma a fortalecer a capacidade de vigilância e a presença do Estado na faixa de fronteira. (LIMA, 2018). O Exército Brasileiro, em seu site de internet, cita o seguinte:

“O Exército, presente na Amazônia desde o início do século XVII, vem ampliando seu dispositivo pela instalação de diversas unidades de fronteira. Tais unidades representam pólos de desenvolvimento, em torno dos quais, como ocorreu no passado, crescem núcleos habitacionais, garantidores da presença brasileira e de nossa soberania.”

É com esse entendimento que se destaca o emprego das diversas unidades de fronteira no combate aos delitos transfronteiriços e ambientais, intensificando a presença militar na faixa de fronteira. Ainda, as ações sociais promovidas pelo Exército Brasileiro, com a finalidade principal de apoio populacional específico, tais como, educação, transporte, evacuação e saúde, dentro de uma comunidade isolada, são grandes ferramentas utilizada atualmente como forma de se manter presente até nas áreas mais remotas do país.

2.2 COMUNIDADES ISOLADAS

Não se tem uma definição que obedeça a um padrão universal, quando se fala em “comunidades isoladas”. Cada país, dependendo de suas particularidades, características e oportunidades, podem até apresentar termos distintos, mas que levam a

conceitos semelhantes.

A Revista DAE (2011) nos direciona ao entendimento de que, as comunidades isoladas são “núcleos habitacionais cuja interligação aos sistemas integrados de abastecimento de água e esgotamento sanitário da zona urbana, seja técnica ou economicamente inviável a curto/médio prazo”. Comunidades isoladas apresentam características que as diferenciam de forma considerável dos núcleos urbanos de maior densidade habitacional, principalmente em relação ao atendimento às suas necessidades, que perpassa as condições sociais e geográficas.

No que se refere a assentamentos humanos isolados, Lannes (2017, p. 24) considera, dentre outras, as variáveis referentes à proporção de pessoas com acesso à eletricidade, a densidade da população e a proximidade a uma cidade como sendo um indicador de acesso a uma vasta gama de serviços. Ainda, nos apresenta o entendimento de que “os Pelotões Especiais de Fronteira são aquartelamentos do Exército Brasileiro, localizados ao longo da faixa de fronteira do Brasil, consistindo, portanto, em comunidades isoladas”, ainda que neste sentido, falte uma definição por parte do Instituto Brasileiro de Geografia e Estatística. (LANNES, 2017, p. 27)

O atendimento às comunidades isoladas, em particular na Região Amazônica, se apresenta como o maior desafio para o alcance dos serviços públicos, dentre eles, o de acesso e distribuição de energia elétrica. Dessa forma, cumpre ressaltar e falar a respeito dos Pelotões Especiais de Fronteira (PEF), enquanto comunidades isoladas e como pontos de desenvolvimento com função estratégica, com possibilidades de ampliação e influência nas comunidades que surgem ao redor.

2.3 PELOTÕES ESPECIAIS DE FRONTEIRA ENQUANTO COMUNIDADES ISOLADAS

A faixa de fronteira amazônica tem sido uma das prioridades da Força Terrestre, devido ao crescente número de delitos transfronteiriços e ambientais, fazendo com que a presença militar na faixa de fronteira se intensifique de forma a não permitir o enfraquecimento da soberania brasileira.

Quanto à segurança na faixa de fronteira amazônica, merece destaque a atuação das Organizações Militares de Fronteira: Companhias, Pelotões e Destacamentos Especiais de Fronteira.

Os Pelotões Especiais de Fronteira (PEF) são elementos avançados que marcam a presença do Exército Brasileiro e do Estado na região. Os PEF têm a missão institucional estabelecida pelas Instruções Provisórias IP: 72-20, que nos traz o entendimento de que as tarefas de um PEF não se limitam apenas a atividades militares em prol da vigilância da fronteira, mas cooperam com a vivificação da área com atividades complementares, tais como a produção, em pequena escala, de gêneros alimentícios de origem vegetal e animal e à prestação de serviços para si próprio e para a comunidade civil existente ao redor do aquartelamento. (BRASIL, MD, 1997)

Estabelecendo-se como uma espécie de vanguarda avançada do Comando Militar da Amazônia (CMA), podemos considerar também que os PEF, compostos em média por cinquenta militares, se distribuem em pontos estratégicos da fronteira, quase sempre localizados à beira dos grandes rios amazônicos, únicos meios de locomoção em superfície e nenhum deles é acessível por estradas. (AGÊNCIA SENADO, 2006)

As regiões fronteiriças na Amazônia são imensidões isoladas, sem comunicação, limitadas em seu desenvolvimento e onde se pode notar uma estrutura dependente, atrelada a atividades de subsistência e elevados custos. Scariot (2007, p.3) nos apresenta aspectos importantes do local, tais como, a carência de infraestrutura de energia, comunicações, transportes e de baixos níveis de produção pela precária tecnologia utilizada na exploração, o que cria um natural sentimento de isolamento, marginalização e exclusão nas populações fronteiriças.

Stochero (2013), em sua matéria jornalística ao portal de notícias G1, narra

algumas das dificuldades encontradas na maioria dos PEF:

"Vinte minutos para abrir uma página na internet. Racionamento de energia elétrica, provida por até 16 horas diárias por um gerador. Sinal de celular, nem pensar. Telefonia fixa? Apenas um orelhão. Água da chuva para beber e água do rio para tomar banho, lavar roupa e louça. Abastecimento de comida e remédio a cada 30 ou 45 dias, dependendo da disponibilidade de um avião."

Baseando-se em entrevista concedida pelo General Eduardo Villas Bôas, Stochero (2013) pontua que a logística na Amazônia é uma dificuldade natural, devido aos meios de transporte serem precários, com rodovias inexistentes e sistema hidroviário por vezes comprometido, pois em grande parte do ano vários rios não são navegáveis. Outro ponto, encarado como fator limitador do poder operativo do PEF, é a questão da energia elétrica, provida por algumas horas do dia através um gerador a diesel. Em 2013, o Exército conseguiu fazer um levantamento da infraestrutura disponível em cada um dos 24 pelotões da Amazônia: no total, havia 38 geradores, mas menos da metade (16) estavam disponíveis para uso. Eles eram de 13 marcas diferentes, o que dificultava a manutenção. (STOCHERO, 2013)

As Forças Armadas vêm suprindo e melhorando essa realidade em algumas áreas. Com ações subsidiárias na região Amazônica, já são notados alguns reflexos no desenvolvimento, nas necessidades e carências locais. Segundo Scariot (2007, p. 21):

"Os Pelotões de Fronteiras do Exército são em muitos pontos os únicos núcleos de civilização. Representam, também, a possibilidade de apoio, educação, transporte, evacuação e saúde (atendimento médico e odontológico), inclusive aos grupos indígenas da região". Contudo, salienta que essa presença é insuficiente diante da grandiosidade da área."

Há a necessidade de uso da infraestrutura dos Pelotões de Fronteira por parte da comunidade local, principalmente no que diz respeito ao acesso à energia elétrica, em particular, provida por geradores a diesel. Surge a necessidade de apresentar meios sustentáveis de geração de energia elétrica, um insumo fundamental para o desenvolvimento da sociedade, visando reduzir o uso de combustível fóssil, proporcionando o uso de uma energia limpa e segura para os PEF e comunidades, suprindo assim as dificuldades logísticas encontradas em manter o gerador a diesel.

2.4 A LUZ SOLAR COMO FONTE DE ENERGIA RENOVÁVEL E SUSTENTÁVEL

Algumas das fontes energéticas mais conhecidas para a geração de energia elétrica são a solar, a eólica, a térmica, a química, a hidráulica e a nuclear. Destacam-se como renováveis, a energia eólica (produzida pela força do vento exercida no "aerogerador", que alimenta um sistema de baterias) e a solar (energia gerada através de placas solares, que funcionam a partir da incidência do sol sobre o painel, produzindo corrente elétrica). Tendo em vista fazer parte do objeto de estudo, será abordada nesse momento, a energia solar.

Segundo Pinho (2008, p. 27):

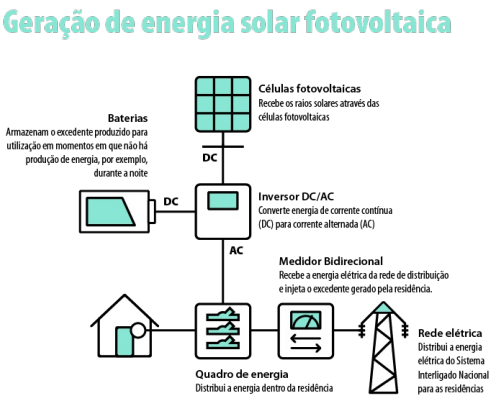
"A energia solar na Terra decorre da incidência dos raios solares na forma de luz e calor e é, na realidade, a origem de todas as outras formas de energia conhecidas. Seu aproveitamento estende-se desde a secagem de produtos até os mais modernos coletores solares planos e parabólicos e os painéis fotovoltaicos. Sua utilização no Brasil ainda é tímida, apesar do potencial solar favorável no território brasileiro, apresentando condições superiores às de muitos países que hoje estão à frente do Brasil em capacidade de potência instalada."

A necessidade de ampliar a matriz energética, de forma a minimizar a dependência de combustíveis fósseis, ganhou importância nos últimos anos e uma possível solução refere-se ao emprego de sistemas de energia solar, em especial a fotovoltaica. Considerando-se a abundância da radiação solar no Brasil, cumpre explorar a aplicação inicial em benefício às comunidades isoladas.

2.5 POTENCIAL DA ENERGIA SOLAR FOTOVOLTAICA NO BRASIL

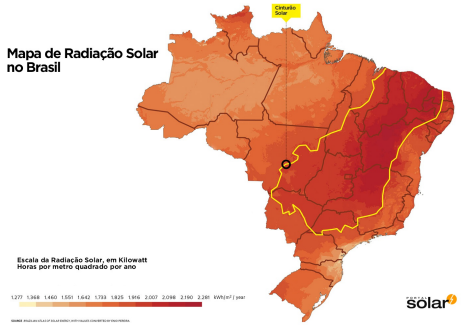
Para a geração de energia fotovoltaica são usados painéis de silício para coletar raios de luz do Sol, que é a fonte renovável de energia mais abundante e amplamente disponível no planeta. É vista como uma tecnologia de energia limpa e sustentável. Cabe um breve entendimento de como funciona a geração de energia solar fotovoltaica, através da Figura 2.

FIGURA 2 : Geração de energia solar fotovoltaica



Dentre as formas renováveis que compõem a matriz elétrica do Brasil, conforme divulgado pela EBC (2017), a energia fotovoltaica é a menos consumida. Constatou-se em 2015 que apenas 0,01% do que foi gerado no país resultou dessa tecnologia. Ainda que pouco utilizada, cumpre dizer que o Brasil possui um potencial gigantesco para aproveitar essa capacidade energética, o que é possível identificar na Figura 3.

FIGURA 3: Mapa de Radiação Solar no Brasil



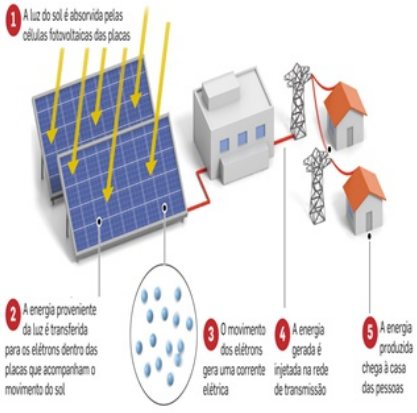
O Portal Solar (2020) observa que mesmo em regiões com menor incidência de radiação solar, o potencial é maior que o da Europa e continua com a informação de que mesmo com menor potencial, a Europa possui instalados mais de 106 GW de energia fotovoltaica, muito superior ao Brasil, que possui um pouco mais de 1 GW instalado. (PORTAL SOLAR, 2020)

As informações referentes à radiação solar de determinada região devem ser analisadas e processadas cuidadosamente, pois um projeto de sistema fotovoltaico depende dessas informações. Isso, para que se torne possível quantificar as necessidades de forma precisa, no intuito de atender ao recurso disponível. Para isso, é possível contar com diversas ferramentas de apoio ao dimensionamento de sistemas fotovoltaicos, a exemplo do serviço web “SunData”, que se destinam ao cálculo da irradiação solar diária média mensal em qualquer ponto do território nacional (CRESESB, 2021).

2.6 SOLUÇÃO ENERGÉTICA PARA OS PEF

Surge como possível solução o emprego do sistema de energia solar fotovoltaica, para minimizar, ou até mesmo sanar o racionamento de energia nos PEF. Nos mercados da tecnologia fotovoltaica existem diversas alternativas de produção de energia, seja para uma residência ou até mesmo uma grande usina solar produzindo energia para milhares de famílias.

FIGURA 4: Usina Fotovoltaica



Fonte: Demape, 2020

Segundo Ribeiro (2013):

“Os mercados de energia solar fotovoltaica em 2017 mostraram um equilíbrio perfeito entre as instalações de grande porte (grandes usinas solares) e a geração distribuída (Sistemas instalados em telhados de casas e empresas), demonstrando essa capacidade única que só a energia fotovoltaica tem de oferecer uma solução para diversas necessidades.”

Tanto as usinas e fazendas solares, quanto os sistemas residenciais mais simples instalados, são opções possíveis de atender à necessidade energética de uma comunidade isolada. É necessário um estudo de viabilidade, considerando os aspectos técnicos, legais, econômico-sociais e ambientais, para decidir dentre as opções disponíveis, sem se esquecer da logística a ser empregada no transporte e na manutenção. Tendo em vista que a manutenção é basicamente limpeza dos painéis solares e periodicamente, a substituição de baterias quando se aplica o sistema Off Grid. Na média os inversores de frequência possuem de cinco a dez anos de garantia, enquanto os painéis solares possuem entre quinze a vinte e cinco anos de garantia da vida útil.

Para o Portal Solar (2020), a usina solar, também conhecida como parque solar, é um sistema solar fotovoltaico de grande porte desenvolvido para a produção e distribuição de energia elétrica. Com foco na distribuição e não no autoconsumo, a usina solar fornece energia em alta tensão, e nesse aspecto se diferenciam dos sistemas fotovoltaicos residenciais.

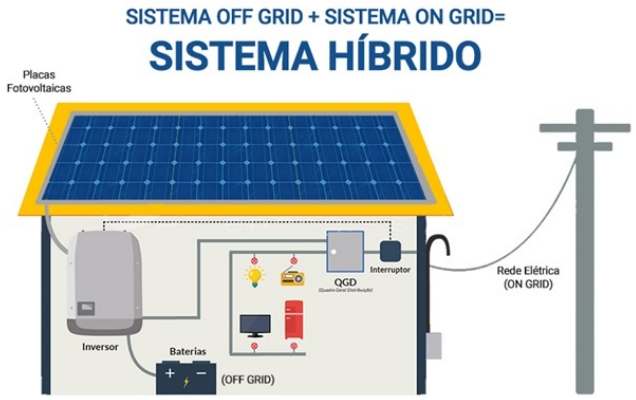
Conforme ilustrado na Figura 4, uma usina solar funciona basicamente da maneira apresentada pelo Portal Solar (2020):

“os painéis solares produzem energia elétrica que passa por um inversor solar para converter esta energia em corrente alternada. A eletricidade produzida pela usina de energia solar é transmitida pelas redes de transmissão de energia e distribuída para o uso em sua casa”.

A outra opção abordada refere-se a um sistema de energia solar fotovoltaico para emprego residencial, que pode ser instalado com ou sem uso de baterias. A possibilidade de uso de baterias responde uma das principais dúvidas, a de como armazenar energia para o consumo noturno. É uma necessidade real dos PEF, além de trazer segurança, também traz comodidade e bem-estar para os militares e famílias desses lugarejos. Além de continuidade aos serviços de comunicações com as bases militares.

É importante diferenciar os sistemas geradores de energia solar com bateria: “híbrido” e “off-grid”. Um gerador solar híbrido com bateria é basicamente a mesma coisa que um gerador solar conectado na rede convencional, mas adicionado um banco de baterias, a exemplo do ilustrado na Figura 2 e Figura 5.

FIGURA 5 : Gerador de Energia Solar Híbrido com Bateria Solar



Fonte: : Portal AWSeNergy , 2021

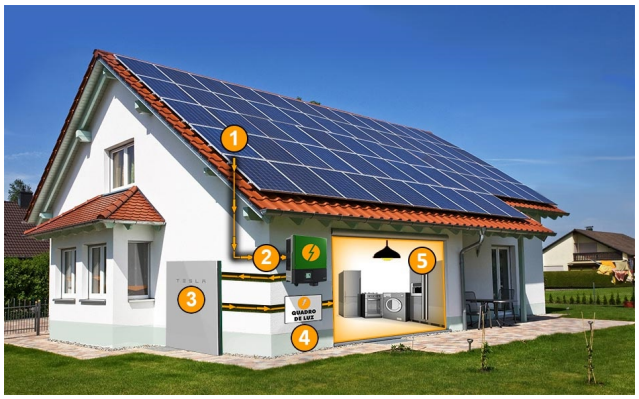
O denominado sistema gerador de energia Off-Grid Solar, ilustrado na Figura 6, é aquele utilizado sem acesso à rede da concessionária local de energia elétrica, de forma que toda a energia produzida através das placas solares é consumida ou armazenada em bateria solar para consumo durante a noite ou quando não houver sol suficiente. Embora ele seja mais simples que um gerador híbrido a quantidade de baterias para energia solar deve ser bem calculada para evitar falta de energia.

No que se refere a aplicação de sistemas fotovoltaicos, Pinho (2008, p. 69) afirma que:

“...em localidades sem o atendimento elétrico convencional, os módulos fotovoltaicos constituem alternativa viável quando comparada com a extensão da rede elétrica, geração a diesel e outras fontes”.

É importante destacar a preocupação com a manutenção preventiva, para garantir o bom funcionamento do sistema.

FIGURA 6: Gerador de Energia Off-Grid Solar



Fonte: Portal Solar, 2020

2.7 CUSTO DE IMPLANTAÇÃO DE UM SISTEMA DE ENERGIA SOLAR OFF GRID.

Ao consultar o valor do óleo diesel em Manaus no valor de R$ 6,809 (Portal Preço dos Combustíveis) sem se ater a itens de manutenção e logística, um gerador de 5KVA ligado pelo período de 16 horas por dia com potência plena, teria anualmente um custo R$ 39.219,84. Ressaltando que esse custo tende a aumentar pois existe a manutenção, o transporte que incrementam esse valor.

Se considerarmos o mesmo cenário, porém agora utilizando um kit de energia solar OFF GRID, o valor de R$ 33.905,23, com uso contínuo por 24 horas, contendo basicamente:

1) 04 und conector mc4 acoplador fêmea;
2) 04 und conector mc4 acoplador macho;
3) 50 mts cabo solar 0,6-1kv 1500v dc preto;
4) 50 mts cabo solar 0,6-1kv 1500v dc vermelho;
5) 01 string box quadro 2 entradas 2 saidas 1000v (1 mppt);
6) 01 inversor solar off grid dc 48v;
7) 01 painel/carre 6kw saida ac 5kva 220v senoidal;
8) 02 estrutura solar;
9) 04 paineis fixador gancho telha colonial smart;
10) 08 painéis solares 460w t;
11) 01 bateria solar litio 48v litio 4.8kwh energia solar;
12) 01 suporte bateria litio kit_bracket hope 4.8l-c1 48v3 48v litio lifepo4 4,8kwh;
13) 01 cabo de conexao bateria hope 4.8 solar litio;
14) 02 estrutura solar;
15) 02 pares perfil smart-x 2,40m.

Diante dos questionamentos inclusive sobre a viabilidade do sistema, vejo que é viável em vários aspectos: extinção da poluição sonora e olfativa ocasionada pelos geradores, economicidade tendo em vista que o valor gasto com geradores de campanha utilizados reduzidos já no primeiro ano e esse valor nos próximos anos poderiam ser investidos em outras áreas, ganhos com o meio ambiente por ser sustentável e ainda para enfatizar a importância do sistema solar nos PEFs, podemos citar o endereço eletrônico da CRESESB SunData, que mostra através de dados a viabilidade em instalar esse sistema renovável. Lembrando que países que possuem menor índice de irradiação solar que o Brasil, aproveitam bem e já se consolidaram nesse meio energético. Alguns questionamentos sobre o funcionamento da energia solar no ambiente amazônico e de fronteira devidos as intempéries, fator característico da região, são respondidos com experiências vividas por todo o mundo. O Brasil como já foi dito, possui um dos maiores índices de irradiação solar e ainda é pouco aproveitado enquanto em outros países que possuem menores índices, já fazem bastante uso dessa tecnologia,

3. CONCLUSÃO

Com a revisão bibliográfica foi possível compreender que nem todas as comunidades podem ser atendidas pela rede convencional de energia elétrica, pois, várias delas situam-se em locais de difícil acesso e sofrem pela falta de serviços essenciais. Nesse sentido, os Pelotões Especiais de Fronteira, estando nas condições de comunidade isolada, suprem a falta da rede convencional de energia elétrica utilizando-se de geradores a diesel, que além do impacto negativo ao meio ambiente, tem seu

uso racionado para economia de combustível, justificado pelo regrado apoio logístico de suprimento, manutenção e transporte.

Barreto (2008) ressalta que:

"O fornecimento de um sistema de geração de energia elétrica em comunidades isoladas deve conter um plano de gestão participativo e sustentável, e devem-se criar estratégias que dêem suporte ao crescimento proporcionado pela chegada da energia elétrica que beneficiem os indivíduos, gerando renda através do uso produtivo da energia."

No intuito de suprir as necessidades energéticas nos PEF, foi apresentada a energia solar fotovoltaica como uma solução viável, por facilitar o acesso à energia elétrica em locais mais remotos. Pinho (2008, p. 76) nos mostra que a energia solar fotovoltaica é uma das principais tecnologias utilizadas para carregar baterias para o atendimento isolado, por ser produzida por uma fonte de energia primária, não utilizar recursos naturais esgotáveis e por não gerar qualquer tipo de efluentes sólidos, líquidos ou gasosos durante o processo de produção da eletricidade, sendo seus impactos restritos ao visual e à ocupação de áreas.

Os sistemas fotovoltaicos têm um conjunto de benefícios e vantagens como poucas fontes de energia podem oferecer, desta maneira e para ratificar essa solução energética, aproveita-se o mencionado por Pinho (2008, p. 30):

"Não se pode, entretanto, excluir a possibilidade de uso das energias renováveis, ainda que com custos de implantação elevados, como é o caso dos sistemas [...] fotovoltaicos, sem considerar os benefícios sociais e ambientais atrelados a eles."

Para a implementação de um sistema fotovoltaico, é necessário um estudo mais aprofundado. A análise da solução mais viável depende do objetivo a ser alcançado e do orçamento disponível, que pode contar com uma solução individualizada, por residência, até uma usina solar com capacidade para atender toda a comunidade isolada que margeia um PEF.

O resultado do levantamento das necessidades impactará significativamente na logística a ser empregada no transporte do material necessário a instalação. Para transportar equipamentos frágeis nessas localidades é necessário o planejamento prévio de uma logística de transporte, levando-se em conta que para chegar a determinados pontos onde não há estradas, pode ser necessário caminhar vários quilômetros, utilizar barco, ou contar com apoio aéreo, quando possível.

Conseguimos observar que o uso dessa energia sustentável, trará continuidade nos serviços e missões com telecomunicações. Pois o exemplo citado faz referência a uma simples residência, porém mesmo aumentando o sistema para abranger outros ambientes e operações, o sistema ainda é mais economicamente viável e sustentável em vários aspectos como poluição, ruído excessivo que pode prejudicar a audição de quem trabalha nas proximidades.

REFERÊNCIAS

BARRETO, Eduardo José Fagundes. et al. Tecnologias de energias renováveis: sistemas híbridos, pequenos aproveitamentos hidroelétricos, combustão e gasificação de biomassa sólida, biodiesel e óleo vegetal in natura. (Soluções energéticas para a Amazônia). Brasília: Ministério de Minas e Energia, 2008. 156 p.

BRASIL, Senado Federal. Agência Senado. Pelotões de fronteira são os braços mais distantes do Exército na Amazônia. jan. 2015. Disponível em: <http://www12.senado.leg.br/noticias/materias/2006/06/02/pelotoes-de-fronteira-sao-osbracos-mais-distantes-do-exercito-na-amazonia>. Acesso em: 07 mai. 2020.

BRASIL, Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. Instruções Provisórias. O Batalhão de Infantaria de Selva. 1ª Edição. 1997. IP 72-20. Capítulo 9 – O BIS sediado em área de fronteira. Artigo III – O Pelotão Especial de Fronteira.

CRESESB. Fontes de dados eólicos e solares. Disponível em: <http://www.cresesb.cepel.br/index.php?

section=com_content&cid=fontes_dados_vento_sol>. Acesso em: 10 mai. 2020

EXÉRCITO BRASILEIRO. Amazônia. Disponível em: <https://www.eb.mil.br/amazonia>. Acesso em: 3 mai. 2020.

FERREIRA, Vagner. Exército Brasileiro e Amazônia: intervenções educativas socio comunitárias, intersubjetividade e tecnologias sociais no 3º Pelotão Especial de Fronteira (3°PEF), em Pacaraima-RR. Americana: Centro Universitário Salesiano de São Paulo, 2016. 134f. Dissertação (Mestrado em Educação). UNISAL – Centro Universitário Salesiano de São Paulo.

IMAZON. Amazônia Legal. Disponível em: <https://imazon.org.br/mapas/amazonia-legal/>. Acesso em: maio 2020

LANNES, Maiza Seabra Nogueira. Sustentabilidade de comunidades isoladas com ênfase em gestão da água, gestão de energia e dimensão psicossocial: os Pelotões Especiais de Fronteira. Brasília, 2017. 305 p.:il. Tese de Doutorado – Universidade de Brasília/Faculdade de Arquitetura e Urbanismo, 2017.

LIMA, Edmar Souto Abreu. Capacidade de Proteção Integrada do Exército Brasileiro na Faixa de Fronteira Amazônica, diante das atuais ameaças existentes nessa região. Orientação: Alexandre Santana Moreira. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2018.

MENIN, José Luis Gonçalves. Ações subsidiárias das Forças Armadas na Amazônia e seus reflexos na segurança e no desenvolvimento. Revista da Escola Superior de Guerra, v.23, n.47, p.21-39, jan/jul. 2007.

MONTE, Leonardo Prado do. Exército Brasileiro na Fronteira Amazônica: Desenvolvimento Regional por Meio de Ações Militares. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/2867/1/Tcc_Inf_Leonardo_Prado_Esao.pdf>. Acesso em: maio 2020.

PINHO, João Tavares. et al. Sistemas Híbridos – Soluções Energéticas para a Amazônia. Brasília: Ministério de Minas e Energia, 2008. 396p

PORTAL MEU GERADOR. Disponível em: <https://meugerador.com.br/kit-energia-solar-off-grid-5kva-220v-368kwp-inversor-growatt-bateria-de-litio-45kwh-90499.html> Acesso em: dezembro 2021

PORTAL Solar. Bateria Solar. Disponível em: <https://www.portalsolar.com.br/bateria-solar.html>. Acesso em: maio 2020.

PORTAL SOLAR. Energia Fotovoltaica. Disponível em: <https://www.portalsolar.com.br/energia-fotovoltaica.html>. Acesso em: maio 2020.

PORTAL SOLAR. Usina Solar no Brasil. Disponível em: <https://www.portalsolar.com.br/usina-solar.html>. Acesso em: maio 2020.

PORTAL SOLAR. Vantagens e Desvantagens da Energia Solar Fotovoltaica. Disponível em: <https://www.portalsolar.com.br/vantagens-e-desvantagens-da-energia-solar.html>. Acesso em: maio 2020.

RIBEIRO, Tina Bimestre Selles. et al. Implementação de Sistemas Fotovoltaicos em Comunidades Isoladas: Reflexões Sobre Entraves Encontrados. Revista Brasileira de Energia, Vol. 19, No. 1, 1º Sem. 2013, pp. 269-283.

SCARIOT, Renato Luiz. O Estado Brasileiro e a soberania na Amazônia. Revista da Escola Superior de Guerra, v.23, n.47, p.21-39, jan/jul. 2007.

REVISTA DAE. Uma publicação da Cia. de Saneamento Básico do Estado de São Paulo. Set. 2011.

ARTIGO CIENTÍFICO

ÁREA DE CONCENTRAÇÃO

EDUCAÇÃO

NOVAS PRÁTICAS NO CURSO AVANÇADO DE ELETRÔNICA DA ESCOLA DE COMUNICAÇÕES NA MODALIDADE DE ENSINO A DISTÂNCIA.

1º TEN CÉSAR DA CONCEIÇÃO CONDE
2º SGT JOSÉ ERLAN NUNES MATIAS

RESUMO: Este artigo visa abordar novas práticas no Curso Avançado de Eletrônica da Escola de Comunicações, na Modalidade de Ensino à Distância (EaD), com a inclusão de ferramentas pedagógicas, antes utilizadas somente na modalidade presencial. Essa temática é de vital importância, pela complexidade do processo educativo, onde houve a necessidade de criar estratégias e atualizações por parte do corpo docente. Em 2017, por determinação do Escalão Superior, houve a redução na carga horária dos Cursos regulares da Escola e para compensar, os cursos passaram a funcionar na modalidade semipresencial, sendo a primeira fase oferecida à distância, aumentando ainda mais os cuidados quanto à preparação do ambiente virtual de aprendizagem e dos recursos pedagógicos a serem utilizados.

Palavras Chaves: EDUCAÇÃO A DISTÂNCIA; NOVAS PRÁTICAS; ENSINO-APRENDIZAGEM.

1 INTRODUÇÃO

O Exército Brasileiro, através do Centro de Educação à Distância, está inserindo nos cursos regulares aprovados por portaria, a modalidade semipresencial, onde parte da carga horária está sendo disponibilizada na fase à distância e a outra parte na fase presencial. Para conseguir disponibilizar materiais e atividades, tem sido utilizado o software livre “Moodle”, que possui muitas ferramentas capazes de dinamizar e aproximar os agentes envolvidos. O ambiente virtual de aprendizagem (AVA), mesmo sendo gratuito, é uma ferramenta poderosa e além da capacidade de oferecer uma gama de possibilidades acadêmicas, pode controlar e fiscalizar tudo o que está sendo realizado dentro da plataforma. É interessante compreender que os regulamentos que regem o ensino no Exército Brasileiro possuem como referência as legislações nacionais e isso traz ao processo de ensino imposições que precisam ser respeitadas para atender as especificidades e referenciais de qualidade para a educação à distância. Com isso, percebe-se o esforço da Escola de Comunicações em oferecer o melhor ambiente virtual possível para seus alunos que, mesmo distantes, conseguem sentir a presença de seus instrutores e monitores nas atividades.

O Decreto no 9.057, de 25 de maio de 2017, que regulamenta a Lei de Diretrizes e Bases da Educação Nacional, cita o seguinte sobre o EaD:

“[...] modalidade educacional na qual a mediação didático-pedagógica nos processos de ensino e aprendizagem ocorra com a utilização de meios e tecnologias de informação e comunicação, com pessoal qualificado, com políticas de acesso, com acompanhamento e avaliação compatíveis, entre outros, e desenvolva atividades educativas por estudantes e profissionais da educação que estejam em lugares e tempos diversos”

Nas últimas décadas, o processo de ensino e aprendizagem tem sido muito influenciado pela popularização das Tecnologias de Informação e Comunicação. A possibilidade de utilização de artefatos tecnológicos nos processos de ensino e aprendizagem sinaliza uma necessidade de repensar e ressignificar as formas de ministrar uma aula.

Na educação à distância, principalmente na forma online, onde as interações basicamente acontecem pela participação dos alunos no AVA, o professor tem mais um

desafio além de repensar as formas de interação, ele precisa saber administrar os diferentes tipos de linguagens, questões relativas à "distância transacional" (distância entre professor e aluno, que não é meramente geográfica, mas educacional e psicológica), tempo e espaço.

O professor, no entanto, continua sendo o mesmo, influenciado muitas vezes por suas experiências no ensino presencial ou outras vezes pelo seu entusiasmo inicial em uma nova modalidade. Porém, somente o entusiasmo não é suficiente. Dúvidas sobre como estruturar uma sala de aula virtual, como otimizar e potencializar os recursos de um AVA ainda permeiam sua prática.

Pensando nisso, apresentaremos neste artigo novas práticas no Curso Avançado de Eletrônica da Escola de Comunicações que contribuirão para a construção mais ativa de um desenho do AVA.

2 DESENVOLVIMENTO

2.1 METODOLOGIAS EXISTENTES

Na procura de novas práticas para proporcionar ao Curso Avançado de Eletrônica da Escola de Comunicações, na fase EaD, metodologias mais ativas, recorreu-se às práticas já empregadas em algumas Instituições de Ensino, em especial, o Instituto Universal Brasileiro e a Loja Burgos Eletrônica.

Fundado em 1941, o Instituto Universal Brasileiro é uma instituição privada pioneira no ensino à distância no Brasil, pela modalidade de ensino por correspondência. Constituiu-se no maior difusor de cursos profissionalizantes à distância do país, no século XX. Por meio de anúncios em jornais e revistas de todo o país, o Instituto chegou a oferecer cerca de 30 tipos de cursos profissionalizantes e supletivos por correspondência. Cursos de eletrônica, mecânica de automóveis, corte e costura e desenho artístico foram alguns dos mais procurados. Desde a fundação até o ano 2000, quatro milhões de pessoas haviam realizado os cursos da escola. A partir do ano 2000, o Instituto Universal Brasileiro também passou a oferecer cursos pela Internet.

O ensino por correspondência, oferecido pelo Instituto Universal Brasileiro, é considerado a primeira geração do ensino a distância (EaD). A segunda geração seria a teleducação e a terceira geração as redes de computadores e as videoconferências.

Além de material impresso acompanhado de kits didáticos, o Instituto dispõe de vários cursos em versão online, proporcionando aos alunos um conteúdo completo, preparado para facilitar a educação à distância.No caso dos cursos em eletrônica oferecidos pelo Instituto, encontrou-se uma metodologia satisfatória de aprendizagem em formato de Curso Apostilado com KIT. Na compra do curso, são enviados aos alunos, pelos correios, kits de eletrônica (material eletrônicos diversos) acompanhados de manual e vídeos didáticos. Com esse material, os alunos podem executar a montagem de várias experiências de circuitos eletrônicos, conciliando os ensinamentos teóricos com o manuseio na prática.

A "Burgos Eletrônica Comércio de CDs, Livros e Componentes Ltda ME" é uma empresa especializada em venda de cursos na área da eletrônica e informática. São oferecidos livros técnicos, videoaulas, Kit Didáticos, esquemas elétricos, manuais de aparelhos e componentes para eletrônica e informática.

Os cursos na área da eletrônica e informática são completamente desenvolvidos por uma equipe encabeçada pelo professor Luís Carlos Burgos, técnico de eletrônica e informática há 25 anos e professor desta área há 19 anos.

No caso dos cursos em eletrônica oferecidos pela Loja Burgos Eletrônica, encontra-se uma eficiente metodologia de aprendizagem em formato de cursos em vídeo por DVDs e cursos com kit didático. Utilizando a idéia do Instituto Universal Brasileiro, na compra do curso, são enviados aos alunos pelos correios, kits didáticos de eletrônica (material eletrônicos diversos), acompanhados de manual e vídeos didáticos. Com esse material, os alunos também poderão executar a montagem de várias experiências de circuitos eletrônicos, conciliando os ensinamentos teóricos com a prática.

2.2 PLANEJANDO ATIVIDADES COM METODOLOGIAS EXISTENTES

Tomando como exemplo as práticas empregadas com sucesso pelo Instituto Universal Brasileiro ao longo dos anos e também as empregadas pela Loja Burgos Eletrônica, a equipe de instrução da Escola, no ano de 2020, inseriu novas práticas no Curso Avançado de Eletrônica da Escola de Comunicações, na modalidade de ensino à distância, com inclusão de ferramentas pedagógicas antes utilizadas somente na modalidade presencial.

Sendo assim, foram criadas no Ambiente Virtual de Aprendizagem (AVA) diversas experiências de eletrônica a serem executadas pelos alunos, utilizando materiais enviados pelos correios e que são devolvidos na apresentação para a fase presencial na Escola, tais como protoboard, fonte de alimentação, componentes eletrônicos, entre outros.

Para essa atividade, os alunos foram orientados a criar um vídeo e adicionar no AVA, demonstrando e explicando os experimentos realizados em protoboard, de acordo com os esquemas disponibilizados pelo tutor. O vídeo pôde ser criado pelo celular ou por outro meio eletrônico e o aluno explicou com a própria fala, narrando o passo a passo no vídeo ou escrevendo em um documento (pdf, word, odt) os procedimentos que realizou nos experimentos. Dessa forma, foi combinada a teoria com os objetivos propostos no Eixo Transversal do curso, onde estão presentes a organização e a coordenação motora. É trivial imaginar, por exemplo, que para um aluno que se propõe a cursar o Avançado de Eletrônica, utilizar um material energizado, mesmo que não ofereça risco por possuir tensão e corrente baixas, é necessária cautela para não queimar algum componente. Ainda, como está sendo empregado um protoboard, o aluno precisa utilizar sua coordenação motora para alinhar os componentes na placa.

Enfim, foi possível criar uma atividade onde todos os processos foram arquitetados, tornando a aprendizagem interativa e eficiente, com discussões em fóruns específicos e, sobretudo, envolvendo aspectos físicos, emocionais e intelectuais.

3 CONCLUSÃO

Adotando a idéia do melhoramento contínuo, a Escola de Comunicações segue buscando novas alternativas para oferecer ao seu público interno e externo o melhor ambiente acadêmico possível, incluindo aí o ambiente virtual de aprendizagem.

Para agilizar esse processo, o EaD precisa ser encarada como um processo contínuo, que busca a todo momento inovar, não só pedagogicamente, mas também quanto a seus recursos tecnológicos e humanos. Uma qualificação que está fazendo parte desse cenário atualmente é o especialista em design instrucional, figura capaz de desenhar um curso com diversas possibilidades de aprendizagem, seria um profissional a ser pensado para fazer parte das instituições de ensino do Exército e contribuir sobremaneira no processo de ensino.

O ambiente virtual de aprendizagem precisa ser utilizado como um espaço de interação. Conhecer e saber aplicar as ferramentas e metodologias previstas nesse espaço também é de fundamental importância para a qualidade e o desenvolvimento do ensino por competências, o qual faz parte das diretrizes do Exército Brasileiro para o Ensino militar.

REFERÊNCIAS

BRASIL. Decreto no 9.057, de 25 de maio de 2017 - Decreto que regulamenta a Lei de Diretrizes e Bases da Educação Nacional. Disponível em:< http://www.planalto.gov.br/ccivil_03/leis/l9394.htm>. Acesso em: 27 de outubro 2019.

BRASIL. Lei nº 9394, de 20 de dezembro de 1996 – Lei de Diretrizes e Bases da Educação Nacional. Disponível em :< http://www.planalto.gov.br/ccivil_03/leis/l9394.htm>.

Acesso em: 28 de outubro de 2019.

BRASIL. Portaria nº 081, de 14 DE MARÇO DE 2017. Cria o Curso Avançado de Eletrônica Boletim do Exército, n. 12, Brasília, p. 15, 24 mar. 2017.

BRASIL. Portaria nº 143 - DECEx, de 25 de novembro de 2014. Aprova as Normas para Desenvolvimento e Avaliação dos Conteúdos Atitudinais (NDACAEB60-N-05.013). Boletim do Exército, n. 51, Brasília, p. 03, 19 Dez. 2014.

BRASIL. Portaria nº 202 - DECEx, de 23 de novembro de 2016. Aprova as Normas para a Avaliação da Aprendizagem – 3ª Edição (NAA – EB60-N-06.004) e dá outras providências. Boletim do Exército, n. 35, Brasília, p. 03, 01 set. 2017.

BRASIL. Portaria nº 549 – CMT EX, de 6 de outubro de 2000. Aprova o Regulamento de Preceitos Comuns aos Estabelecimentos de Ensino do Exército (R-126).

BRASIL. Portaria nº 900 – CMT EX, de 20 de julho de 2015. Cria e ativa o Centro de Educação a Distância do Exército, e dá outras providências. Boletim do Exército, n. 30, Brasília, p. 07, 28 ago. 2015.

NETTO, Carla. Interatividade em ambientes virtuais de aprendizagem. In: Educação Presencial e Virtual: espaços complementares essenciais na escola e na empresa. FARIA, Elaine Turk (Org.) Porto Alegre: EDIPUCRS, 2006.

SÁ, Iranita M. A. Educação a Distância: Processo Contínuo de Inclusão Social. Fortaleza, 1998.

SCHERER, S.; BRITO, G. S. Educação a Distância: Possibilidades e Desafios para a Aprendizagem Cooperativa em Ambientes Virtuais de Aprendizagem. Educar em Revista (Impresso), v. 4, p. 53-77, 2014.

MENEZES, Ebenezer Takuno de. Verbete Instituto Universal Brasileiro. Dicionário Interativo da Educação Brasileira - Educabrasil. São Paulo: Midiamix, 2001. Disponível em: <https://www.educabrasil.com.br/instituto-universal-brasileiro/>. Acesso em: 22 de abr. 2020

ARTIGO CIENTÍFICO

ÁREA DE CONCENTRAÇÃO

INFORMÁTICA

UM COMPARATIVO ENTRE FERRAMENTAS DE SCANNER DE VULNERABILIDADES

2º SGT HUMBERTO PEREIRA DIAS

RESUMO: Aplicações Web têm sido produzidas sob grande demanda atualmente, e a acirrada concorrência do mercado de produção de software aliada a complexidade de desenvolvimento, trouxe à tona, o surgimento de brechas de segurança e crescimento de vulnerabilidades no cenário mundial. Por consequência, a necessidade de buscar equilíbrio perfeito entre disponibilidade e segurança, ocasionou uma crescente produção de ferramentas de escaneamento de redes, que visam expor a quem o utilize, todas as vulnerabilidades do ambiente testado. Portanto, a credibilidade dos resultados das ferramentas de scanner tornou-se algo de grande valia. Logo, este artigo propõe um comparativo entre ferramentas que realizam esse tipo de serviço, altamente requisitados nos dias atuais.

Palavras Chaves: REDES DE COMPUTADORES. SEGURANÇA. VULNERABILIDADE.

1 INTRODUÇÃO

A internet tornou-se indispensável à grande maioria da população. Ela é utilizada para realizar diversas atividades do dia a dia, tais como: fazer transações bancárias, compras online, redes sociais, entre outras atividades. O alto grau de conectividade além de grandes benefícios inseriu em ambientes virtuais incidentes que comprometem a segurança das redes, fazendo com que massivos investimentos em ferramentas de proteção contra invasores acompanhem este crescimento (KUROSE, 2006).

Para Nakamura e Geus (2007), ambientes de redes, quando não bem configurados, podem apresentar falhas passíveis de ataques internos ou externos que podem comprometer o seu bom funcionamento, tornando-o mais lento e acessível às pessoas não autorizadas, através da exploração de vulnerabilidades, que são bugs na implementação. Ataques exploram ‘brechas’ existentes em qualquer nível relacionado à proteção da informação que são: sistema operacional, serviços e protocolos, rede e telecomunicações, aplicação, usuários e organização (NAKAMURA; GEUS, 2007).

Para estruturação de um ambiente de rede seguro é preciso analisar alguns pontos básicos na configuração das políticas de segurança. Estas, por sua vez, fornecem um conjunto de regras, leis e práticas destinadas à gestão da segurança. Criptografia, assinatura digital, autenticação e controle de acesso são alguns dos mecanismos utilizados para implementação destas políticas, pois provém um conjunto de ferramentas gerenciáveis (DUMONT, 2006).

Às ferramentas citadas anteriormente, pode-se somar ainda os sistemas de detecção de intrusão (IDS) que monitoram o tráfego da rede, e equipamentos de restrição e controle de tráfego como firewall, utilizados para reforçar a segurança e deixar o ambiente mais seguro. De acordo com Kurose (2006), proteger a comunicação e os recursos da rede é o fator primordial para definir uma comunicação segura. Sendo assim, a segurança da rede não envolve apenas sua proteção, mas também a detecção de falhas, ataques à infraestrutura e reações a serem tomadas. O monitoramento das ameaças torna-se necessário para que se detectem mudanças na rede. Através de scanners detectores de vulnerabilidades é possível realizar diversos testes na rede e procurar falhas de segurança. Os Scanners são programas de varredura de rede utilizados para detectar vulnerabilidades em sistemas, sua funcionalidade consiste em procurar por

falhas de segurança na rede para corrigi-las antes que sejam exploradas por intrusos, obtendo alguma vantagem ou causando prejuízo (MOREIRA et al., 2008).

O presente artigo tem como objetivo principal, apresentar um comparativo entre softwares de varredura de redes de computadores com ênfase nas suas funcionalidades principais.

2 DESENVOLVIMENTO

Apesar da existência de inúmeros scanners, que tem como objetivo detectar vulnerabilidades de sistemas Web, estudos demonstram que há disparidade entre as ferramentas existentes em termos de abrangência e níveis de exploração das vulnerabilidades [Rocha et al. 2012, Doup´e et al. 2010, Vieira et al. 2009].

A função de monitoramento continuo em aplicações e dispositivos, em busca de pontos vulneráveis, além de reportar esses erros em detalhes, demonstra a importância da escolha certa do scanner de rede para atuar em ativos da iniciativa pública ou privada. Sendo assim, é possível a escolha perfeita de "um" scanner dentre os disponíveis no mercado? Ou a escolha certa, se daria por um conjunto de ferramentas de scanner, para se ter um resultado fidedigno das análises de vulnerabilidades?

2.1 HIPÓTESE

Em face da disparidade entre as ferramentas de scanner, no que diz respeito às suas funções e capacidades, a melhor escolha seria por um conjunto de ferramentas que se complementam.

2.2 OBJETIVO GERAL

O presente artigo tem como objetivo principal, apresentar um comparativo entre softwares de varredura de redes de computadores com ênfase nas suas funcionalidades principais.

2.3 OBJETIVOS ESPECÍFICOS

Identificar e corrigir brechas em sistemas que possam comprometer sua funcionalidade, desempenho e segurança;

Alterar e melhorar a configuração de softwares visando torná-los mais seguros e eficientes;

Visualizar e implantar novas soluções de segurança de acordo com as necessidades encontradas;

2.4 JUSTIFICATIVA

Analisar vulnerabilidades não é atacar um sistema, mas sim realizar verificações de portas para conhecer possíveis aplicações e atualizações identificando falhas e vulnerabilidades. Segundo Willie e David (2013), há muitas soluções para a análise de vulnerabilidade, os principais são o Nessus e o OpenVAS que são usados para fazer a varredura em busca de vulnerabilidades, o OpenVAS (Sistema de Avaliação de Vulnerabilidade Aberto), é um excelente programa utilizado na avaliação de vulnerabilidades, sendo este uma ramificação do projeto Nessus. Uma característica importante do OpenVAS é o fato de ser gratuito, além de ser parte do conjunto de aplicações instaladas na distribuição Kali Linux. Para a análise de vulnerabilidades, com estes softwares, é preciso a instalação e configuração de servidor OpenVas e de um cliente, que pode ser qualquer computador, que possua acesso via navegador a este servidor. Com este sistema em funcionamento é possível analisar todos os sistemas conectados em rede. Para Muniz e Lakhani (2013), a análise só será útil desde que o profissional de segurança tenha conhecimento de como realizar o cálculo dos riscos de cada problema encontrado, bem como fornecer o custo esperado para reduzir esses riscos. Cabe a ele decidir se o risco associado à vulnerabilidade encontrada justifica o gasto necessário para reduzi-la a um nível aceitável. Para tal decisão utiliza-se um modelo de cálculo que estima o impacto e a probabilidade da vulnerabilidade a ser explorada, e então calculam-se e analisam-se os riscos. Por riscos,

a norma ISO/IEC Guide 73:2002,12 define como: “A combinação da probabilidade de um evento e suas consequências”. Por Vachek (2009).

2.5 REFERENCIAL TEÓRICO

Segundo Nakamura e Geus (2007, p. 56) “A defesa é mais complexa do que o ataque”, pois, para o atacante, basta que ele consiga explorar um ponto de falha da organização. Para embasar a proposta deste artigo fez-se necessário um levantamento teórico de aspectos relevantes ao tema, os quais são apresentados nesta seção, iniciando pelo levantamento sobre conceitos básicos de segurança, vulnerabilidades e trabalhos correlatos.

Caso uma determinada técnica não funcione, ele pode tentar explorar outras, até que seus objetivos sejam atingidos. Já para as organizações, a defesa é muito mais complexa, pois exige que todos os pontos de ataque sejam defendidos. A falta de conhecimento sobre as vulnerabilidades do próprio sistema e os mecanismos apropriados de defesa geram várias falácias relacionadas com a problemática da segurança. Algumas falácias são: “tenho um firewall, então meu sistema está seguro” ou “meu sistema é totalmente seguro”. Na verdade, negligenciar um único ponto de defesa faz com que todos os esforços dispensados na segurança dos outros pontos sejam em vão se este ponto vulnerável for descoberto e explorado. Profissionais mal qualificados tendem a mal dimensionar ou ignorar as reais fragilidades e supervalorizar os dispositivos de segurança implementados. Com isso, a 12 organização passa a correr riscos ainda maiores, que são o resultado da negligência dos profissionais responsáveis. Isso acontece, comumente, com os firewalls ou antivírus, que podem não proteger a organização contra diversos tipos de ataques. (WHITAKER; NEWMAN, 2005).

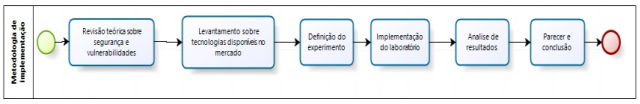
Novas tecnologias trazem consigo novas vulnerabilidades e é preciso ter em mente que novas vulnerabilidades surgem diariamente. O aumento da conectividade resulta em novas possibilidades de ataques visto que a facilidade de acesso traz como consequência o aumento de novos curiosos. Entender a natureza dos ataques é fundamental. Muitos ataques são resultado da exploração de vulnerabilidades que podem ser uma falha no projeto ou na implementação de um protocolo, aplicação, serviço, sistema. Erros de configuração e administração de recursos computacionais e falhas humanas também geram brechas de segurança (NAKAMURA; GEUS, 2007).

Em particular, alguns fatores, como a utilização de serviços remotos e as frequentes atualizações de software fazem com que as redes sejam mais vulneráveis ao passo que ferramentas maliciosas estão tornando-se a cada dia, mais simples e mais acessíveis. (WHITAKER; NEWMAN, 2005).

2.6 METODOLOGIA

Este estudo vislumbra, a partir de uma relevante pesquisa bibliográfica sobre o tema vulnerabilidade e também um levantamento técnico de mercado sobre ferramentas para análise deste tipo de falha, apresentar elementos que permitam a um administrador de ambientes computacionais reduzir o risco agregado a seus equipamentos, processos e infraestrutura. (Dantas, Marcus,2011). O infográfico representado na Figura 3 apresenta as etapas adotadas para a pesquisa.

FIGURA 1 - Etapas adotadas na pesquisa



Fonte: Autor

Para alcançar o objetivo delineado será realizado um conjunto de experimentos com os scanners de vulnerabilidades Nessus e OpenVas, a fim de solucionar as dúvidas sobre qual software apresenta melhor desempenho em diferentes aspectos. Em um laboratório de pesquisa será implementado um cenário contendo um conjunto de computadores conectados em uma rede local, a partir daí será feita a análise dos computadores com as ferramentas e a comparação dos resultados obtidos. Foi feita uma comparação entre o Nessus e o OpenVas de forma qualitativa, levando-se em conta as seguintes

características: Facilidade de instalação; Disponibilidade para sistemas operacionais; Custo da instalação; Facilidade de operação do sistema; Facilidade de identificar o problema e as possíveis soluções pelo relatório obtido na análise e; Analisar a importância da vulnerabilidade destacada pelo scanner.

Esta seção apresenta dois trabalhos correlatos relacionados ao tema de pesquisa descrito neste artigo. O estudo publicado "Nessus/OpenVASComparison Test" em 2009 pelo Laboratory for Systems and Signals (LSS) apresenta os resultados obtidos por meio de testes realizados em seu ambiente de rede. Neste experimento a análise de vulnerabilidades foi realizada por dois scanners, onde os níveis de vulnerabilidades de 15 diferentes servidores foram avaliados em pleno ambiente de produção, este artigo apresenta uma proposta parecida, mas usouse as ferramentas versão 2013 e um ambiente de teste menor, com apenas utilizando apenas computadores com o sistema operacional Windows. A pesquisa intitulada "Audit System at CESNET-CERTS", por Vachek (2009), relata técnicas de auditoria em sistemas baseadas em servidores Linux e ferramentas de análise de vulnerabilidade a fim de apresentar um modelo efetivo de auditoria.

Para a realização dos experimentos deste estudo implementou-se, um laboratório feito a partir de quatro máquinas virtuais, utilizando virtual box rodando sistemas operacionais Windows 7 logicamente conectados por meio da rede NAT. Dois dos sistemas desta rede foram analisados pelo Open VAS e o Nessus, em tempo de produção.

O intuito do experimento está na identificação das vulnerabilidades inerentes aos sistemas e que podem ser identificadas pelas aplicações de monitoramento. Para que os testes fossem o mais próximo possível da realidade, foram simuladas diferentes situações, como um sistema real em produção, a fim de obter uma precisão válida dos resultados. Algumas das tarefas realizadas, durante o monitoramento foram: assistência remota, conexão e permissões a compartilhamentos e serviços web e acesso a um servidor WAMP (Windows, Apache, MySQL, PHP). A plataforma de testes estava baseada no Sistema Operacional Windows, tendo como variantes as versões: Windows 7 e Windows XP. A adoção do Windows se justifica pela sua utilização em grande escala em ambientes de pequenas e médias empresas.

Os resultados das comparações dos testes estão representados na Tabela 1, a justificativa para cada resultado pode ser observado na tabela 2, nesta se encontram as características avaliadas nos programas. Tabela 1. Itens avaliados e suas respectivas notas de acordo com os programas. (TABELA NO ANEXO A).

Os tópicos referentes a Tabela 1 foram avaliados de acordo com a sua importância utilizando-se os símbolos ++ e --, simulando a utilização em uma empresa de pequeno e médio porte. As comparações (A) e (D) tem menos relevância, comparadas com as demais, pois no cenário do experimento, a empresa tem poucos computadores e o tempo gasto a mais ou não, tanto para instalação quanto para operação do sistema não faria uma grande diferença. O tópico (B) é relevante pois o Nessus está disponível para Windows e Linux, enquanto o Open Vas só pode ser executado no Linux, vale lembrar que nesse caso basta ter o Linux, que em geral é gratuito, instalado. O tópico (C) é muito importante para o nosso cenário já que o valor gasto com o Nessus para uma empresa com muitos ou poucos computadores seria o mesmo. Da mesma forma o Open Vas é gratuito independentemente da quantidade de computadores. Os tópicos (F) e (G) são os de maior relevância pois vão decidir a qualidade da análise e correção das vulnerabilidades e o tempo gasto para isso. (Beal, Adriana.2005).

3 CONCLUSÃO

Após análise dos scanners Open Vas e Nessus, verificou-se que a importância dos softwares de varredura de vulnerabilidades em ambientes corporativos é vital, posto que falhas de segurança, podem facilmente

comprometer toda a estrutura e organização de uma instituição. O comparativo entre os softwares supracitados, deixou clara, a necessidade de trabalho em conjunto das ferramentas, mesmo com a diferença em termos de resultados não tenha sido substancial. É de se notar que foi comparado um software de código aberto com um proprietário, e o ambiente de teste e o cenário adotado simulam uma organização de pequeno porte, com um número pequeno de computadores conectados e em produção. Logo, diante dos resultados obtidos, conclui-se que em se tratando de segurança, não se pode haver brechas, e a pequena diferença de resultados obtidos através da utilização de ambos os softwares demonstram que houveram resultados diferentes, o que sugere que a utilização isolada não cobriria todo o necessário para se ter uma rede o mais segura possível.

ANEXO A – RESULTADOS DAS COMPARAÇÕES DOS TESTES

Cod	Itens Avaliados	Avaliação Nessus	Avaliação OpenVas	Justificativa Nessus	Justificativa OpenVas
A	Facilidade de Instalação	++	+_-	Seu download é rápido e pode ser feito no site oficial do programa; sua instalação também é rápida, porém, há a necessidade de um cadastro online, o que atrasa a instalação; possui uma interface gráfica intuitiva; por fim os tutoriais para instalação podem ser encontrados no site do software	Download também pode ser feito no site oficial; sua instalação é complexa, pois é preciso configurar em linhas de comando, apesar disso houve facilidade de encontrar tutoriais contendo scripts que facilitam o processo de instalação
B	Disponibilidade para sistemas operacionais	++	+-	Cliente/Servidor rodam em todas as plataformas: Linux, Windows e Mac OS X	O Servidor só tem suporte para Linux, porém o cliente pode ser acessado pelo browser em todos os sistemas operacionais
C	Custo de instalação	--	++	O Nessus é um software pago custa em torno de $1500,00 por ano, mas cota com uma versão gratuita com algumas limitações como por exemplo o uso em apenas algumas redes locais.	É um software livre com a licença sob licença GPL.
D	Facilidade de operação do sistema	++	+-	Fácil operação á tem uma seleção de testes prontos com conjuntos de pluguins selecionados para diferentes tipos de cenários	Apresenta interface gráfica, sua configuração é mais completa porém o usuário tem mais liberdade para escolher o modelo de varredura, e modificar todos os pluguins.
E	Facilidade de identificar o problema e as possíveis soluções pelo relatório obtido na análise	+-	+-	Gera um relatório apresentado as vulnerabilidades encontradas e lis para atualizações que possam resolver os problemas.	Também apresenta relator, contendo as vulnerabilidades e links para possíveis atualizações que possam resolver o problema.
F	Analisar a importância da vulnerabilidade destacada pelo scanner	+-	++	Foram analisadas 12 vulnerabilidades de médio e alto risco não identificou uma vulnerabilidade grave sobre o servidor que poderia garantir ao atacante acesso remoto a	Encontrou 16 vulnerabilidade de médio e alto risco.

REFERÊNCIAS

ABNT. NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da Informação. Rio de Janeiro: ABNT, 2005.

Alencar, G.Dias; Queiroz, A. Lira; Queiroz, R. J. Guerra Barretto. Um Fator Ativo na Segurança da Informação. IX Simpósio Brasileiro de Sistemas de Informação, João Pessoa, PB: UFPB, 2013.

ALVES, Maria Bernardete Martins; ARRUDA, Suzana Margret de. Como elaborar um Artigo Científico. Disponível em: <http://www.bu.ufsc.br/design/ ArtigoCientifico.pdf>. Acesso em: 18 maio 2017.

BEAL, Adriana. Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BAUER, C. A. Política de segurança da informação para redes corporativas. Trabalho de conclusão de curso – Centro Universitário Feevale, 2006.

BRASIL. Tribunal de Contas da União. Boas Práticas de Segurança da Informação/ Tribunal de Contas da União. 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

BORGES, A. Ataque de fixação de sessão. Revista Linux. 2014. Disponível em: < http://www.linux-magazine.com.br/images/uploads/pdf_aberto/LM_92_14_15_02_colalexborges.pdf >. Acessado em: 2 Jun. 2014.

BROWN, T; GALITZ, G. O farejador de vulnerabilidades OpenVAS. Linux Magazine, São Paulo, , Abr. 2010.

Dantas, Marcus. Segurança da Informação: uma abordagem focada em gestão de riscos, Livro Rápido, 2011.

GALEGALE, Gustavo Perri e Col. Internet das Coisas aplicada a negócios - Um estudo bibliométrico. Revista de Gestão da Tecnologia e Sistemas de Informação. v. 13, no 3, Set/Dez., 2016, pp. 423-438. Disponível em: <http://www.jistem.fea.usp.br/index.php/jistem/article/viewFile/10.4301%25S 1807-17752016000300004/616>. Acesso em: 18 maio 2017.

GONÇALVES, Adriana Aguillera. A proteção do conhecimento e a inovação na Universidade Estadual de Londrina. 2012. Dissertação (Mestrado em Gestão da Informação) - Universidade Estadual de Londrina, Londrina. Disponível em: <http://repositorio.utfpr.edu.br/jspui/handle/1/337>. Acesso em:18 maio 2017.

MORAES, A. F. de. Redes de computadores: fundamentos. 7. Ed. São Paulo: Editora Érica, 2010.

MOREIRA et al. Scanners de Vulnerabilidades Aplicados a Ambientes Organizacionais. Revista Eletrônica da Faculdade Metodista Granbery: Jul/Dez, 2008. 63

MORENO, D. Tipos de PenTest. Disponível em: < http://www.100security.com.br/tipos-de-pentest/ >. Acessado em: 7 Mai. 2014.

NAKAMURA, E. T.; GEUS, P. L de. Segurança de redes em ambientes cooperativos. São Paulo: Novatec Editora, 2007.

ARTIGO CIENTÍFICO

ÁREA DE CONCENTRAÇÃO

GESTÃO

SISTEMA DE GERENCIAMENTO DE ESTOQUE: IMPLEMENTADO POR LEITOR RFID COM ARDUINO

2º TEN JEFFERSON ADINIZ BORGES FERREIRA
2º SGT ISAIAS LUCAS BUENO

RESUMO: A otimização do processo de gerenciamento, manutenção e estoque de material classe VII com eficiência é missão de alguns setores do Exército brasileiro. Visando resolver este problema foi feito um experimento que apresenta um sistema de gerenciamento de estoque por leitor RFID utilizando arduino com capacidade de gravação e leitura de dados por rádio frequência nas etiquetas, auxiliando o controle de estoque com o histórico de manutenção dos rádios e baterias fornecendo transparência ao processo.

Palavras Chaves: IOT, GERENCIAMENTO, RFID, ARDUINO.

1 INTRODUÇÃO

A manutenção e gerenciamento do material classe VII do Exército Brasileiro são de responsabilidade do Centro Logístico do Centro de Comunicações e Guerra Eletrônica do Exército (CLog/CCOMGEX), Centro Integrado de Telemática do Exército (CITEX) e dos Parques Regionais de Manutenção e dos próprios detentores em 1o escalão. As OMs de mais alto escalão de manutenção possuem estoques de suprimentos para a realização destas manutenções, tais como antenas, baterias, etc; estes não podem permanecer por tempo indeterminado em estoque, sendo necessário um controle rigoroso, tanto devido ao seu custo quanto à sua vida útil.

São diversas as tecnologias aplicadas ao controle desse tipo de material, normalmente determinada, por cada responsável, dentro de sua esfera de atribuições. Dessa maneira, possui-se um grande número de sistemas diferentes atuando com o mesmo propósito.

Ter essa quantidade de sistemas dificulta a interação entre os bancos de dados das Organizações. O que poderia diminuir essa dificuldade é a implementação de fluxos de suprimentos mais consistentes, confiáveis e integrados.

Uma solução para essa diversidade de sistemas seria a aplicação de um sistema único para controle de todo esse tipo de material, juntamente a uma tecnologia de conferência e rastreio de objetos, sendo que esta fosse ágil, de fácil implementação, e que suporte as condições por vezes severas que a atividade militar exige.

RFID, do inglês: Radio Frequency Identification, ou seja, Identificação por Radiofrequência é uma tecnologia de comunicação sem fio capaz de identificar objetos ou pessoas por meio da utilização de etiquetas de identificação única.

A utilização da tecnologia RFID se difundiu bastante nos últimos anos devido à redução de seu custo e de melhorias em seu funcionamento. Atualmente a tecnologia está sendo utilizada em diversas áreas, sendo as principais: cadeias de abastecimento, segurança e rastreio de objetos (WEINSTEIN, 2005).

Um sistema RFID é composto por três componentes básicos: etiqueta, leitor e um servidor, podendo conter mais de uma etiqueta e mais de um leitor (HUNT; PUGLIA; PUGLIA, 2007). Mesmo parecendo moderno, não é de hoje que Exércitos utilizam comunicação sem fio para dentificação de objetos; durante a Segunda Guerra Mundial os britânicos usavam um sistema de RADAR

que captava as ondas eletromagnéticas dos aviões que permitia a sua localização. Com esse sistema, os Britânicos identificavam a localização dos aviões inimigos e a sua velocidade. Com essas informações, previam como antecipar os ataques Alemães e alertavam a população a fim de que se protegesse. (SANTINI, 2008).

Em junho de 2003 a empresa multinacional WalMart fez um anúncio que impulsionou a tecnologia Radio frequency identification(RFID). A empresa exigiu que até janeiro de 2005, seus 100 maiores fornecedores teriam que adicionar uma etiqueta RFID a todas as caixas enviadas para qualquer centro de distribuição da WalMart (LOCKTON; ROSENBERG, 2006). Essa exigência, além de ter proporcionado o crescimento do mercado de RFID, proporcionou também a criação de padrões na produção das etiquetas e leitores, reduzindo seus custos e consequentemente viabilizando a sua utilização por empresas de menor porte.

WANG et al., 2006, realiza um estudo de caso que demonstra a utilização de um projeto RFID em um hospital em Taiwan com o intuito de ajudar a supervisionar e identificar os casos de uma doença chamada Severe Acute Respiratory Syndrome (SARS), altamente infecciosa que desafiou as medidas de contenção nos hospitais das regiões afetadas. A implementação do projeto exigiu a participação de especialistas nas áreas de saúde e da tecnologia, sendo necessária a construção de uma etiqueta própria para coletar as medições de temperatura dos pacientes, de modo a identificar os casos da doença sem comprometer a saúde dos funcionários, o que demonstra também uma possível aplicação da tecnologia na área da saúde em controle de doenças contagiosas.

A tecnologia RFID veio, como toda inovação, melhorar segmentos da indústria, pecuária, logística, saúde, entre outros. Ela ajuda a evitar roubos, gerir inventários, aumentar a produtividade, entre outros, mas também possui algumas desvantagens. O uso da tecnologia RFID no controle de estoques reduz bastante as possibilidades de erros e melhora a precisão dos dados do estoque. Com as etiquetas inteligentes presentes nos itens é possível ter o controle preciso de todos os itens em estoque, até mesmo em tempo real.

Vantagens:

- Prevenção de roubos e falsificação de mercadorias;
- Contagem instantânea do estoque;
- Capacidade de armazenamento, leitura e envio de dados;
- Não necessita de proximidade do leitor para reconhecimento dos dados;
- Precisão nas informações e velocidade de envio;
- Localização de itens;
- Otimização de processos de gestão, (aumento da velocidade dos processos e eliminação dos erros humanos);
- Durabilidade de etiquetas com possibilidade de reutilização.

Desvantagens:

- Invasão de privacidade;
- Má interação com metais, (pode ser contornado através de encapsulamentos);
- Processamento e Energia, (devido à necessidade de um maior processamento dependendo da aplicação a bateria não se mostra suficiente).

Em comparação com os códigos de barras, a utilização da tecnologia RFID apresenta um número bem maior de vantagens como apresentado na Figura 1, porém o maior empecilho de sua adoção é o seu alto custo de implementação (MICHAEL; MCCATHIE,2005). Os principais benefícios trazidos por essa tecnologia são: escaneamento sem linha de visão, redução de mão de obra e melhoria do controle do estoque e da visibilidade das mercadorias podendo monitorá-las a todo instante.

TABELA 1 - Tabela de vantagens da tecnologia RFID em comparação ao código de barra.

CÓDIGO DE BARRAS	RFID
Necessita linha de visão para ser lido	Pode ser lido sem linha de visão
Pode ser lido apenas individualmente	Pode ler várias etiquetas simultaneamente
Não pode ser lido se estiver danificado ou sujo	Pode lidar com ambientes agressivos ou sujos
Pode identificar apenas o tipo do item	Pode identificar um item específico
Não pode ser atualizado	Novas informações podem ser gravadas
Exigem rastreamento manual	Pode ser rastreado automaticamente

Fonte: White, 2007

Uma das características mais atrativas é o escaneamento sem linha de visão, ou seja, as etiquetas RFID podem ser lidas sem serem visualizadas podendo estar em qualquer disposição, desde que estejam dentro do alcance do leitor. Com isso, por exemplo, é possível identificar todo o conteúdo de uma caixa sem ter que abri-la. Além disso, os leitores conseguem escanear múltiplas etiquetas simultaneamente, o que permite, juntamente com as outras características de escaneamento, automatizar o processo de identificação e contagem de mercadorias.

RFID vem ganhando grande espaço no desenvolvimento de sistemas de automação e robótica no mundo inteiro. Dentre suas funcionalidades explora-se neste artigo alguns sinais coletados a partir de sensores, que são capazes de inserir informações, que facilitarão o controle de estoque e da manutenção dos equipamentos classe VII do Exército Brasileiro.

Desse modo a busca por meios tecnológicos de maneira a otimizar o controle dos processos de manutenção que são submetidos os equipamentos a rádio. Os principais objetivos a serem alcançados na implementação de tais tecnologias visam diminuir o tempo ocioso do material em manutenção e obter dados como histórico de manutenção dos equipamentos, do controle patrimonial e da transparência do processo.

2 DESENVOLVIMENTO

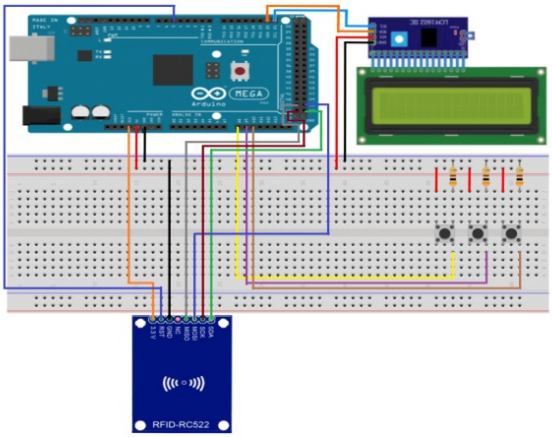
Foi realizada uma pesquisa bibliográfica sobre os temas: IoT, Sistemas de gerenciamento, RFID, Leitor RFID, arduino e material classe VII . Depois um experimento de validação projetando um sistema de leitura, de gravação e de controle de RFID utilizando arduino.

2.1 MATERIAIS UTILIZADOS:

- Arduíno MEGA 2560;
- Módulo de RFID RC522;
- Botão de Push-Button;
- Display 16x2 IC2;
- Protoboard;
- Resistor 300 Ω (Ohms);
- Jumpers;
- Cabo USB para Interface PC;
- Computador.

O esquema mostra a ligação do módulo RFID ao Arduino utilizando três botões para seleção das funções de leitura de ID TAG, leitura e gravação.

FIGURA 1 - Esquemático de montagem do circuito eletrônico RFID Arduino.



Fonte: Projeto Interdisciplinar Eletrônica, EsCom 2020.

1. Cadastro das baterias no sistema Arduino de gerenciamento de estoque com a tecnologia de etiquetas e/ou cartões de RFID;
2. Inserção dos dados – por meio do computador conectado ao Arduino - referentes a data de entrada das baterias no sistema e última recarga;

3. Estocagem das baterias devidamente identificadas no depósito;

4. Quarenta e oito horas antes de completar o ciclo semestral de recarga, o sistema emitirá alertas visuais através do LED do sistema de gerenciamento, informando a respeito da necessidade de recargas das baterias em estoque;

5. Vinte e quatro horas antes de completar o ciclo semestral de recarga, o sistema emitirá alertas visuais e sonoros, através do LED e do buzzer ligados ao sistema de gerenciamento, informando a respeito da necessidade de recargas das baterias em estoque;

6. Verificação, no display do sistema de gerenciamento, pelo responsável qual bateria deverá ser recarregada em seu ciclo semestral de calibração;

7. Calibração e recarga de até 40% das baterias com o tempo de 6 meses em estoque;

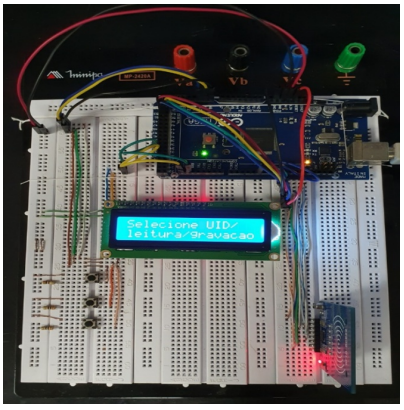
8. Inserção de nova data de calibração das baterias já inseridas no sistema;

9. Estocagem das baterias de acordo com as normas de armazenamento das mesmas, apresentadas no item 2 da seção Generalidades;

10. Retornar ao item 4, enquanto as baterias estiverem em estoque.

11. O sistema montado do arduino conforme o esquemático de ligação pode ser visto a seguir:

FIGURA 2 - Leitura da ID TAG do Cartão.

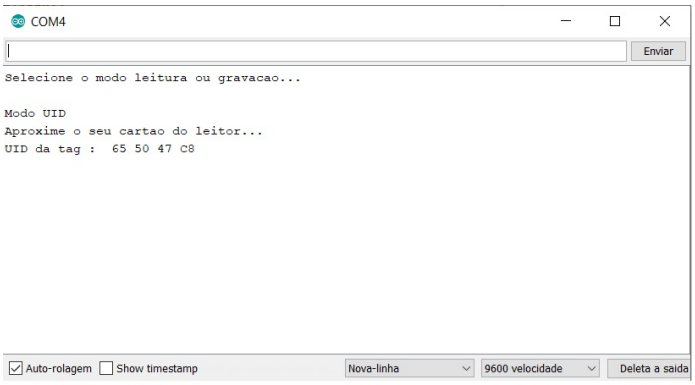


Fonte: Projeto Interdisciplinar Eletrônica, EsCom 2020.

2.2 RESULTADOS E DISCUSSÃO

Foi efetuada a leitura da ID TAG do cartão, pressionando o push-button e selecione o “Modo de leitura ID”. Depois disso, aproximando o cartão do Leitor de RFID e os dados foram mostrados no display LCD e também no Monitor Serial.

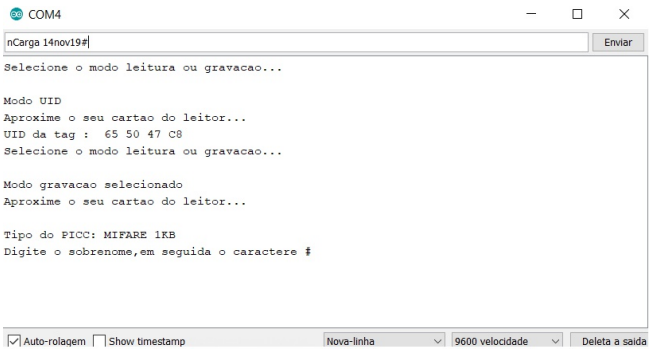
FIGURA 3 - Leitura da ID TAG do Cartão.



Fonte: Projeto Interdisciplinar Eletrônica,EsCom 2020.

Selecionando o Modo de Gravação, pressionando o push-button responsável e mantendo o cartão próximo ao Leitor de RFID até o final da gravação. Posteriormente digitando a informação da data da última carga realizada nas baterias dentro do Monitor Serial, terminando com o caractere #. Ex: nCarga 14Nov19 #Repitindo o mesmo processo, agora para o número de lote. Ex: nLote 003#

FIGURA 4 - Gravação dos Dados.

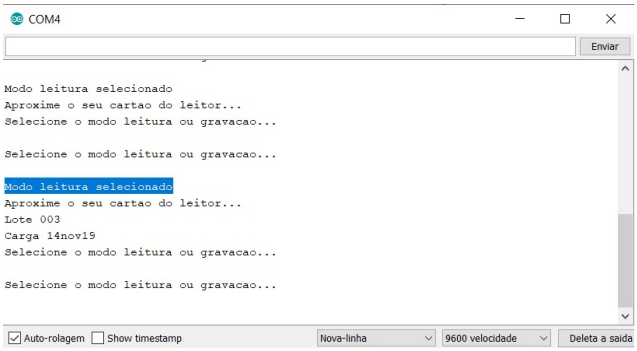


Fonte: Projeto Interdisciplinar Eletrônica,EsCom 2020.

Quando a gravação ocorre normalmente, a mensagem “Gravação OK!” é exibida no display LCD. Para efetuar a leitura, foi pressionado o push-button e selecionado o “Modo de Leitura”.

Depois disso, aproximou-se o cartão do Leitor de RFID e os dados foram mostrados no display LCD e também no Monitor Serial.

FIGURA 5 - Leitura dos Dados.



Fonte: Projeto Interdisciplinar Eletrônica,EsCom 2020.

3 CONCLUSÕES

Este trabalho demonstrou, utilizando um experimento, a possibilidade de um sistema de gerenciamento de estoque implementado por leitor RFID em arduino, com capacidade de gravação, leitura e controle de estoque especificamente para o material classe VII do Exército Brasileiro.Esse sistema de automação pode servir de apoio e controle as comunicações, auxiliando no gerenciamento equipamentos e obter dados como histórico de manutenção, de controle patrimonial e de transparência do processo. Uma situação ideal seria um a interligação de um sistema gerenciador de material classe VII com banco de dados dentro da rede interna do exército.

REFERÊNCIAS

EXÉRCITO BRASILEIRO. Normas administrativas regulativas ao material de Comunicações e Guerra Eletrônica.EB80–N–75.001. Brasília: Departamento de CiÊncia e Tecnologia, 2019.

WEINSTEIN, R. Rfid: A technical overview and its application to the enterprise. IEEE, 2005.

D.; PUGLIA, A.; PUGLIA, M. RFID: A Guide to Radio Frequency Identification. [S.l.]: John Wiley & Sons, Inc., 2007.

SANTINI, Arthur Gambin. RFID: Conceitos, Aplicabilidade e Impactos. 1.ed. Rio de Janeiro: Ciência Moderna Ltda, 2008.

WANG, S.-W. et al. Rfid applications in hospitals: a case study on a demonstration rfid project in a taiwan hospital. IEEE, 2006.

MICHAEL, K.; MCCATHIE, L. The pros and cons of rfid in supply chain management. IEEE, 2005.

NUNES, Rodrigo; Microcontrolador MSP430 Parte III (MIC094). Disponível em:< www.newtoncbraga.com.br>. Acesso em: 14 de Maio de 2020.

OLIVEIRA, Claudio Luís Vieira. Arduino de 2020.

BRASIL. Projetos Interdisciplinares dos alunos do curso Avançado de Eletrônica. Exército Brasileiro, Brasília: Escola de Comunicações, 2019.

ARTIGO CIENTÍFICO

ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

SERVIÇO DE RADIOAMADOR EM AÇÕES DE DEFESA CIVIL NO BRASIL

ADRIANO RIBEIRO PACHECO

RESUMO: Com o advento da internet e da telefonia celular, esperava-se que a comunicação por meio de rádio transceptor, entre cidadãos co- muns, caísse em desuso. Mas, não foi o que aconteceu. Tudo isso por conta de que, a comunicação via rádio oferece a oportunidade de se relacionar e formar comunidades com valo- res próprios, como a satisfação de prestar assistência em situações extremas. A função social e a prestação de serviços são algumas das principais virtudes funcionais do radioamador. É, de certa maneira, reconhecido o importante papel desempenhado pelos radioamadores de todo o mundo, principalmente, em situações de emergência e catástrofes. As comunicações de radioamador são das mais confiáveis em circunstancias extremas, em consequência das vulnerabilidades que o sistema de comunicações, hoje existente, constitui. Surge no Brasil a Rede Nacional de Emergência de Radioamadores – RENER, uma importante reserva nacional de comunicações, usada em situações de calamidade, desastre natural, ameaça à vida e à integridade do cidadão, em apoio à Defesa Civil. Através deste artigo, baseado em revisões bibliográficas, livros, periódicos e em legislações nacionais, é possível se divulgar mais o serviço prestado pelos radioamadores, com as suas capacidades voluntariosas de mobilização, de intervenção, e ainda de capacidades técnicas e atuação junto à defesa civil.

Palavras Chaves: COMUNICAÇÕES DE EMERGÊNCIA; DEFESA CIVIL; GERENCIAMENTO DE CRISES; RADIOAMADOR ; RADIOCOMUNICAÇÃO.

1 INTRODUÇÃO

A probabilidade de desastres naturais ou por ação humana aumenta gradativamente, e isso pode ser atribuído a vários fatores, como por exemplo as interferências do homem na natureza utilizando a tecnologia que avança em grande velocidade e começa a permear cada aspecto da vida. Hoje, a tecnologia está mais prontamente disponível para qualquer um, criando um ambiente altamente hostil e com uma maior probabilidade de desastre acidental ou intencional.

Imediatamente após um desastre, a capacidade de disseminar a informação é essencial. Planejar e se preparar para desastres exige tempo, e de certa forma tempo bem gasto, principalmente no que se refere a comunicações de emergência. A capacidade de coordenar esforços de resgate, de combater incêndios, de evacuar áreas em perigo iminente, dentre outros, é impedida quando a comunicação é perdida.

Tomando como base os conceitos sobre o Serviço de Radioamador e sobre o papel da Defesa Civil, este artigo visa apresentar, através de revisões bibliográficas, os meios legais e formas de emprego das comunicações de radioamador em situações de emergência. Para isso se faz necessário conhecer mais de perto o Serviço de Radioamador, as suas capacidades de mobilização e intervenção; e ainda, conhecer os aspectos legais e de que forma se dá a sua importante atuação em ações de defesa civil no Brasil.

1.1 ABORDAGEM SOBRE O RÁDIO TRANSCEPTOR

Coube, nesse artigo, tratar de rádio transceptor passando, inicialmente, um pouco pela história do rádio. A criação do rádio é um assunto polêmico, que considera os três possíveis responsáveis: Guglielmo Marconi, o

primeiro a patentear uma tecnologia de radiotransmissão; Nikola Tesla, que patenteou diversas tecnologias utilizadas nos projetos de radiotransmissão de Marconi; e o padre, brasileiro, Roberto Landell de Moura que, segundo registros, teria realizado a primeira radiotransmissão, no começo da década de 1890, antes mesmo do registro de patente de Marconi. Para Rodrigues (2009):

A invenção do rádio é creditada ao inventor e cientista italiano Guglielmo Marconi, nascido em 1874 na cidade de Bolonha. Desde menino demonstrando interesse pela Física e Eletricidade, Marconi foi o primeiro a dar explicação prática aos resultados das experiências de laboratório anteriormente realizadas por Heinrich Hertz, Augusto Righi e outros. Pelos resultados dos estudos de Hertz, Marconi concluiu que tais ondas poderiam transmitir mensagens, e, assim, em 1895, fez suas primeiras experiências, com aparelhos rudimentares, na casa de campo de seu pai. Conseguiu fazer chegar alguns impulsos elétricos a mais de um quilômetro de distância.

Mas, Alencar (2020) defende que:

O padre Roberto Landell de Moura construiu o primeiro transmissor sem fio para a transmissão de mensagens, em 1892, alguns anos antes de Marconi começar seus primeiros testes na Itália. Em 1894, ele realizou a primeira transmissão pública por meio de ondas hertzianas, entre o alto da Avenida Paulista e o alto de Sant'Anna, em São Paulo, cobrindo uma distância de oito quilômetros. Entre 1903 e 1904, Landell de Moura conseguiu, nos Estados Unidos, as patentes de três inventos: o transmissor de ondas (hertzianas ou landellianas), o telefone sem fio e o telégrafo sem fio.

De qualquer maneira, a radiotransmissão é uma tecnologia que se desenvolveu e caracterizou durante o século XX. Sua primeira contribuição para a comunicação foi a eliminação da necessidade de fios para a troca de mensagens. Para todas as aplicações de radio frequência (RF) é necessário, no mínimo, um par de comunicadores, ou seja, o emissor e o receptor. Um sistema de rádio é composto por duas estações de rádio, pelo menos, sendo uma transmissora e outra receptora (BRAGA, 2015).

Conforme abordado por Braga (2015), um radiotransmissor é um aparelho que produz ondas eletromagnéticas ou ondas de rádio, agregando-lhes informações como, por exemplo, na forma de código telegráfico ou do som de um microfone. A radiotransmissão depende de um transmissor, que converte os sinais sonoros em ondas eletromagnéticas, e de um receptor, que decodifica o sinal eletromagnético. Existem também os equipamentos que unem as duas funções, chamados de transceptores, e foram adotados no começo do século XX por radioamadores, que utilizavam a tecnologia para transmitir comunicados e para realização de conversas informais. A tecnologia também foi utilizada na comunicação de soldados na Primeira Guerra Mundial (1914), onde o rádio permitiu a instalação muito mais rápida das comunicações, a alcances mais longos e distantes, do que era possível com telefones de campo.

No começo da década de 1920, os radioamadores começaram a montar as primeiras emissoras, que transmitiam notícias e fonogramas, e se multiplicavam rapidamente. A repercussão dessas transmissões foi tão grande que iniciou a comercialização de equipamentos receptores e surgiram as primeiras emissoras comerciais de rádio em 1922.

2 O SERVIÇO DE RADIOAMADOR

Radioamador ou radioamadora é a pessoa habilitada pelo governo para operar uma estação de radiocomunicações amadora. No Brasil o órgão responsável pela regulação do Serviço de Radioamador é a Agência Nacional de Telecomunicações – Anatel, a qual aponta o seguinte conceito:

O Radioamadorismo é o serviço de telecomunicações de interesse restrito, destinado ao treinamento próprio, intercomunicação e investigações técnicas, levadas a efeito por amadores, devidamente

autorizados, interessados na radiotécnica unicamente a título pessoal e que não visem qualquer objetivo pecuniário ou comercial. (ANATEL, 2020).

O Serviço de Radioamador no Brasil é concedido pelo Governo às pessoas habilitadas. Assim sendo, para ser radioamador, o cidadão deve ser autorizado pelo Governo Federal, conforme o Regulamento do Serviço de Radioamador, aprovado pela Resolução nº 449, de 17 de novembro de 2006. Já a atribuição das frequências e as condições de uso do serviço foram aprovados pela Resolução nº 697, de 28 de agosto de 2018, complementada pelo Ato nº 9106, de 22 de novembro de 2018 (ANATEL, 2020).

Antes da obtenção da outorga do Serviço de Radioamador, se faz necessária a obtenção do Certificado de Operador de Estação de Radioamador (COER), que conforme presente no Inciso II, do Art. 4º, do Regulamento do Serviço de Radioamador, "é o documento expedido pela Anatel à pessoa física que tenha comprovado ser possuidora de capacidade técnica para operar estação de radioamador". Para obtenção do COER é necessária a aprovação em testes de avaliação, cujas matérias variam de acordo com a classe do COER: Classe C, Classe B e Classe A.

2.1 EVOLUÇÃO E ASPECTOS LEGAIS DO SERVIÇO DE RADIOAMADOR

A origem do radioamadorismo remonta ao interesse individual de operadores isolados e dispersos pelos Estados Unidos da América (EUA) em seguir as primeiras experiências com o rádio no início do século XX. Segundo Maxim (1930), os radioamadores despertaram para o fato de que havia muitos deles espalhados pelo EUA após a Lei Federal do Rádio, de 13 de agosto de 1912, a qual reconhecia o radioamadorismo no país, alocando essa comunidade abaixo da faixa de frequência dos 200 metros, pouco consideradas para comunicações comerciais e militares. A Lei fornecia um Livro de Chamadas (Call Book) que continha os nomes de todos os radioamadores que haviam passado nos testes necessários para garantir a licença de transmissão.

O número impressionante listado neste livro foi uma revelação, pois mostrou que, em vez de alguns pesquisadores individuais isolados, haviam milhares de radioamadores altamente entusiasmados nos Estados Unidos. Entende-se o Call Book como a primeira rede para tráfego de mensagens entre estações radioamadoras, que posteriormente se organizaram e fundaram a American Radio Relay League (ARRL).

Em 1925 foi organizado o primeiro congresso internacional, englobando 23 nações e formando a União Internacional de Rádio Amador, em seu termo original International Amateur Radio Union (IARU). Até então, muitos países desconheciam a atividade e mesmo proibiam o serviço. Conforme consta no site da IARU:

A IARU foi fundada em uma reunião em Paris em 1925 como representante internacional do movimento Radioamador. Na época, as "ondas curtas" estavam apenas começando a ser compreendidas e exploradas para a comunicação global usando níveis de potência e antenas que estavam ao alcance de indivíduos que operavam em suas próprias casas. Esses radioamadores precisavam de uma organização para coordenar suas atividades e ser sua voz em conferências internacionais. (IARU, 2020).

No Brasil, o surgimento do radioamadorismo se deu, de forma oficial, em 5 de novembro de1924, quando o Diário Oficial da União publicou o decreto n.º 16.657 (atualmente revogado), regulamentando as estações, até então clandestinas. Hoje, o Serviço de Radioamador é regulamentado pela Resolução nº 449, de 17 de novembro de 2006. A resolução tem por objetivo disciplinar as condições para execução do Serviço e a obtenção do Certificado de Operador de Estação de Radioamador (COER).

Quanto ao aspecto de que o serviço de radioamador é de caráter voluntário e não visa vantagem pecuniária ou comercial qualquer, aumenta a sua importância para atividades de Defesa Civil, de acordo com entendimento de Neto (2007):

O voluntariado exerce extrema importância para o sucesso de uma Defesa Civil. É com o auxílio de trabalhos voluntários

que o Estado presta serviços concernentes às atividades de defesa civil com maior facilidade. O profissional, de qualquer área, que é voluntário da Defesa Civil, além de estar exercendo a cidadania, está contribuindo para que os problemas existentes em sua comunidade sejam resolvidos. (NETO, 2007).

Desse modo, é possível compreender como uma rede para comunicações de emergência, formada exclusivamente por voluntários, faz parte do Sistema Nacional de Proteção e Defesa Civil (SINPDEC), se colocando à disposição do interesse público quando da ocorrência de desastres.

2.2 A IMPORTÂNCIA DO RADIOAMADORISMO PARA A DEFESA CIVIL

Ainda que pouco conhecido pela sociedade em geral, é excessivamente e reconhecido o importante papel desempenhado pelos radioamadores em situações de emergências. O sistema de comunicações hoje existente constitui ainda uma das vulnerabilidades do sistema nacional de proteção e socorro, e as comunicações de radioamador se apresentam como das mais confiáveis em circunstancias extremas, como endossado por Colossi, Archangelo e Medeiros (2020):

Algumas estações de radioamador trabalham com grande autonomia, com fontes alternativas de energia elétrica, equipamentos portáteis e exercem comunicações ponto a ponto, sem fios, sem intermediações, com um pessoal experiente e motivado pelo voluntariado. Por isso são essas estações e cidadãos os potenciais promotores de comunicações auxiliares às autoridades e população em apuros. Os radioamadores brasileiros têm constantemente mostrado seu valor social no tráfego de mensagens que tratam de desaparecidos, busca por remédios ou informações sobre parentes distantes. Nas enchentes em Pedro Osório (RS) e em Blumenau (SC, 1983), nas áreas isoladas com centenas de desabrigados, lá estavam os radioamadores com suas estações portáteis para colaborar e manter as comunicações emergenciais. (COLOSSI; ARCHANGELO; MEDERIOS, 2020).

O radioamadorismo é de importância fundamental no apoio a Defesa Civil, com o objetivo de suprir os meios de comunicações usuais quando os mesmos não puderem ser acionados, em razão de desastre, situação de emergência ou estado de calamidade pública.

De acordo com o Sistema Nacional de Proteção e Defesa Civil (SINPDEC), “defesa civil é o conjunto de ações de prevenção e de socorro, assistenciais e reconstrutivas, destinadas a evitar ou a minimizar os desastres, preservar a integridade física e moral da população, bem como restabelecer a normalidade social”.

Ao conhecer mais de perto as atividades desenvolvidas pelos radioamadores, com as suas capacidades voluntariosas de mobilização, de intervenção, e ainda de suas capacidades técnicas, foi possível promover, pelos órgãos competentes, a sua plena integração também no Sistema Nacional de Proteção e Defesa Civil. Desta forma, foi criada a Rede Nacional de Emergência de Radioamadores – RENER, pela Portaria Ministerial MI-302, de 24 de outubro de 2001, publicada no Diário Oficial da União n º 201, Seção I, de 26 de outubro de 2001. De acordo com a Portaria, em seu Art. 1º:

§ 1° A REDE tem a finalidade de prover ou suplementar as comunicações em todo o território nacional, quando os meios usuais não puderem ser acionados, em razão de desastre, situação de emergência ou estado de calamidade pública.

§ 2° Poderão participar da REDE, em caráter voluntário, pessoas físicas portadoras do Certificado de Operador de Estação de Radioamador – C.O.E.R., bem como as estações de rádio detentoras de Licença de Radioamadores, expedida pela Agência Nacional de Telecomunicações – ANATEL.

§ 3° A REDE NACIONAL DE EMERGÊNCIA DE RADIOAMADORES

– RENER, será ativada e subordinada operacionalmente à Secretaria Nacional de Defesa Civil – SEDEC e supervisionada pela

Confederação de Radioamadorismo – LABRE, podendo, também, vir a ser ativada, parcialmente, nos Estados e Municípios, pelas Coordenadorias Estaduais de Defesa Civil – CEDEC e pelas Comissões Municipais de Defesa Civil – COMDEC, respectivamente, de comum acordo com as Federações da LABRE, estaduais.

§ 4º Tendo em vista que o serviço a se provido pela REDE relativo às comunicações, cuja eficiência pressupõe rigorosa observância a princípios e normas legais já estabelecidas, fica criado no âmbito do Ministério da Integração Nacional, Grupo de Trabalho que terá a incumbência de elaborar a Norma de Ativação e Execução dos Serviços a serem prestados pela REDE. (BRASIL, 2001)

Num país de dimensões continentais como o Brasil, a necessidade de sistemas de comunicação instantâneos, não convencionais, é de extrema importância (JARDIM, 2012). Levando ao conhecimento de que por este motivo, foi criada uma rede de radioamadores para auxiliar os órgãos oficiais de salvamento, resgate e prevenção a calamidades, a RENER.

2.3 O SISTEMA NACIONAL DE PROTEÇÃO E DEFESA CIVIL

De acordo com a Constituição Federal de 1988, as ações de proteção e defesa civil são de competência dos três Entes da Federação. Porém, são pouco mencionadas, e apenas dois artigos são encontrados com assuntos pertinentes à defesa civil na Carta Magna: os arts. 22, inc. XXVII, e 144, § 5º, da Constituição Federal (BRASIL,1988). É possível inferir que todas as políticas públicas acerca das ações de gestão de riscos devem ser criadas pela União. As ações de proteção e defesa civil são regidas pela Lei nº 12.608, de 10 de abril de 2012, a qual "institui a Política Nacional de Proteção e Defesa Civil - PNPDEC, dispõe sobre o Sistema Nacional de Proteção e Defesa Civil - SINPDEC e o Conselho Nacional de Proteção e Defesa Civil - CONPDEC, e autoriza a criação de sistema de informações e monitoramento de desastres e dá outras providências", conforme consta em seu Art. 1º. A Cartilha de Defesa Civil e Prevenção de Desastres (Gestão 2017-2020), pontua que "o SINPDEC, vinculado ao governo federal por meio do Ministério da Integração Nacional, deve apoiar os Entes da Federação com o poder de mobilizar a sociedade civil para atuar em desastres, coordenando o apoio logístico para o desenvolvimento das ações de proteção e defesa civil".

O SINPDEC também estabeleceu as competências de proteção e defesa civil em âmbito local, na qual está presente, dentre outras, a competência municipal de mobilizar e capacitar os radioamadores para atuação na ocorrência de desastre.

2.4 ASPECTOS JURÍDICOS E ATRIBUIÇÕES DOS RADIOAMADORES INTEGRANTES DA RENER

O Radioamador, ao longo dos tempos, tem demonstrado a importância das comunicações. Principalmente, quando chamado para ajudar em situações nas quais o seu serviço, humanitário e voluntário, seja colocado à disposição das autoridades e em benefício da população. Países como Estados Unidos da América, Japão, México, Espanha, Colômbia, Argentina, para citar alguns, possuem Redes de Emergência de Radioamadores, integradas com as autoridades competentes.

O Brasil, conta com a Rede Nacional de Emergência de Radioamadores – RENER, uma importante reserva nacional de comunicações, criada pela Portaria Ministerial MI-302, de 24 de outubro de 2001, com o objetivo de suprir os meios de comunicações usuais, quando os mesmos não puderem ser acionados, em razão de desastre, situação de emergência ou estado de calamidade pública. Cabe ressaltar que a RENER faz parte do Sistema Nacional de Proteção e Defesa Civil (SINPDEC), regido pela mencionada Lei Federal nº 12.608/2012.

O Ministério da Integração, criando a RENER e colocando a Liga de Amadores Brasileiros de Rádio Emissão - LABRE como coordenadora da operação conjunta Defesa Civil e Radioamadores reconhece, oficialmente, o valor dos radioamadores brasileiros.

Em 22 de julho de 2009, foi aprovada a Norma de Ativação e Execução dos Serviços

da Rede Nacional de Emergência de Radioamadores – RENER, através da Portaria Min nº 307. Segundo a portaria, a RENER poderá ser ativada nos estados e municípios afetados por desastres, através das Coordenadorias Estaduais de Defesa Civil - CEDEC e das Comissões Municipais de Defesa Civil - COMDEC, apoiadas pela LABRE. Conforme consta na Norma de Ativação:

Um radioamador devidamente cadastrado na RENER, presente em um local de desastre, poderá ativar a rede independente de instruções superiores. No caso de ativação da Rede Nacional de Emergência de Radioamadores – RENER, somente os radioamadores pertencentes à Rede poderão fazer uso das frequências previamente designadas e, em caráter excepcional, qualquer outro radioamador, desde que o faça com a finalidade precípua de transmitir uma informação útil para aquele momento. (BRASIL, 2009).

A RENER submete-se à fiscalização, prevista em lei, pela Anatel, que juntamente a LABRE, as Estações Coordenadoras Federal, Estadual e Municipal deverão ser comunicadas sobre a ativação e o término de qualquer rede de emergência, pelo responsável por sua ativação.

Cabe ressaltar que, os radioamadores voluntários cadastrados na RENER devem ser treinados nos seguintes assuntos básicos: comunicações de emergência, tráfego dirigido de mensagens pela rede ou repetidor, conhecimento técnico e ética operacional, para respostas aos desastres. Com a observação de que pelo menos, uma vez ao ano, a estação Coordenação Federal promoverá a realização de uma operação simulada de resposta a desastres.

2.5 RENER: MOBILIZAÇÃO NA TRAGÉDIA DA REGIÃO SERRANA DO RIO DE JANEIRO

Radioamadores sobem a Serra para tentar estabelecer comunicação remota com Nova Friburgo-RJ, conforme publicação do Jornal O GLOBO, por Isabela Bastos, em 12 de janeiro de 2011:

RIO - Isolada por terra depois dos temporais que caíram na noite de ontem e com as comunicações por telefone fixo e celular interrompidas, Nova Friburgo depende, no momento, do trabalho de radio-amadores para se comunicar com o resto do Rio. Oito operadores de estação de rádio- amador estão auxiliando, em esquema de revezamento, a Defesa Civil daquele município, em auxílio aos sistemas de comunicação oficiais, que entraram em colapso com as chuvas e a falta de energia.

Segundo o coordenador estadual da Rede Nacional de Emergência de Rádio Amadores (Rener), vinculada à Secretaria Nacional de Defesa Civil, Carlindo Norberto Oliveira, uma equipe com oito rádio-amadores subiu a serra, na manhã e tarde desta quarta-feira, para montar duas estações provisórias de comunicação.

A equipe, dividida em três veículos com tração nas quatro rodas, rumou para Friburgo com o objetivo de se aproximar ao máximo da cidade, que está com todas as estradas interrompidas por quedas de barreiras.

- Não existe forma de se chegar por terra, no momento, a Friburgo, e a comunicação por telefone fixo e celular inexiste. O sistema de comunicação da Defesa Civil local está com problemas e estamos auxiliando. Oito radio-amadores da cidade estão auxiliando às autoridades públicas. Mas o serviço está sendo feito em revezamento porque eles dependem de baterias que já estão acabando. A equipe que subiu a serra foi incumbida de montar uma base de comunicação no meio do caminho e outra o mais perto possível da cidade - explicou Carlindo.

A equipe que vai tentar estabelecer uma fonte de comunicação com Friburgo está preparada para passar a noite na serra. Segundo o coordenador estadual da Rener, os rádio-amadores são pessoas com experiência em sobrevivência em situações adversas.

Isolada e incomunicável, Nova Friburgo dependeu basicamente de operadores de estação de radioamador, integrantes da RENER, que auxiliaram, em esquema de revezamento, a Defesa Civil do município.

Uma equipe de radioamadores, com experiência em sobrevivência em situações adversas, também subiu a serra para montar estações provisórias de comunicação, com o objetivo de se aproximar o máximo possível da cidade.

3 CONCLUSÕES

No decorrer do trabalho foi possível responder ao problema quanto aos aspectos legais e de que forma se dá a importante atuação do Serviço de Radioamador em ações de Defesa Civil no Brasil. Com a oportunidade de conhecer, de for- ma sucinta, a história do radioamadorismo, que começou com os experimentos do padre Ro- berto Landell de Moura e do italiano Guglielmo Marconi, onde estabeleceram as primeiras transmissões de rádio no final do século XIX e início do século XX. Surgindo, então, o radioa- mador como a pessoa dedicada ao estudo e desenvolvimento das telecomunicações.

Houve o entendimento de que o radioamadorismo se mantém como um Serviço de Telecomunicação, regulado no Brasil pela Anatel, e reconhecido pela União Internacional de Telecomunicações. Também, foi possível verificar a existência de uma rede de emergência, a RENER, formada por radioamadores voluntários, treinados, e devidamente autorizados que, com seus equipamentos, se colocam à disposição do interesse público quando acontecem desastres ou nas ações de prevenção dos mesmos.

No apoio a Defesa Civil, tem importante emprego, com o objetivo de suprir os meios de comunicações usuais, quando os mesmos não puderem ser acionados, em razão de desastre, situação de emergência ou estado de calamidade pública. Sobremaneira, a existência de um parque relativamente independente dos serviços habituais de telecomunicações garante importância estratégica em situações de emergência, calamidade pública ou até mesmo crise militar.

Por fim, é notável que, ao longo da história da radiocomunicação perpetuou-se a tradição de auxílio e de solidariedade, que se tornaram fundamentos do espírito do radioamadorismo. Todo radioamador, seja qual for a sua classe, deve estar consciente de que sua estação, a qualquer momento, e por algum tempo, pode ser o único elo de comunicação entre um desastre e as autoridades competentes.

O autor é Monitor da Escola de Comunicações do Exér- cito Brasileiro. Graduado em Administração Pública – UNISUL. Pós-Graduado em Segurança Privada – UNI- SUL. Pós-Graduado em Segurança, Planejamento e Res- posta de Emergência em Eventos de Grande Porte – UNYLEYA. Pós-Graduado em Logística da Cadeia de Su- primentos – Faculdade de Tecnologia Senac. Pós-Gradu- ando em MBA Executivo em Gerenciamento de Crises – UNYLEYA. Pode ser contactado pelo e-mail: adria- no.pck@gmail.com.

REFERÊNCIAS

ALENCAR, Marcelo S., LOPES, Waslon T. A., ALENCAR, Thiago T. O fantástico padre Landell de Moura e a transmissão sem fio. Disponível em: < http://memoriallandelldemoura.org/wp- content/uploads/2018/11/O-Fant%C3%A1stico-Padre-Landell-de-Moura.pdf>. Acesso em: 26 mar. 2020.

ANATEL. Veja os procedimentos para obtenção do Certificado de Radioamador. Disponível em: <https://www.anatel.gov.br/setorregulado/ra dioamadorismo>. Acesso em: 28 mar. 2020.

BASTOS, Isabela. Rádio-amadores sobem a Serra para tentar estabelecer comunicação remota com Nova Friburgo. Jornal O GLOBO Rio, 12/01/2011. Disponível em:< https://oglobo.globo.com/rio/radio- amadores-sobem-serra-para-tentar-estabelecer-comunicacao-remota-com-nova-friburgo-2839358>. Acesso em:12 mar. 2020.

BRAGA, Newton C.. Transmissores – Volume 1. 2ª edição. Instituto Newton C Braga. São Paulo - Brasil – 2015

BRASIL. Constituição (1988). Constituição [da] Republica Federativa do Brasil. Brasília:

Senado Federal, 1988.

BRASIL. Lei nº 9.608, de 18 de fevereiro de 1998. Dispõe sobre o serviço voluntário e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, nº 35, p. 2, 19 fev. 1998. Seção 1.

BRASIL. Ministério das Comunicações. Agência Nacional de Telecomunicações. Resolução nº 449, de 17 de novembro de 2006. Aprova o Regulamento do Serviço de Radioamador. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, nº 230, p. 79-82, 1 dez. 2006. Seção 1.

BRASIL. Portaria Ministerial MI-302, de 24 de outubro de 2001. Regula os meios de comunicações usuais, quando os mesmos não puderem ser acionados, em razão de desastre, situação de emergência ou estado de calamidade pública. Diário Oficial [da] República Federativa do Brasil, Brasília, 26 out. 2001. Seção 1.

BRASIL. Portaria Ministerial MI-307, de 22 de julho de 2009. Aprova a Norma de Ativação e Execução dos Serviços a serem prestados pela Rede Nacional de Emergência de Radioamadores - RENER. Diário Oficial [da] República Federativa do Brasil, Brasília, 22 jul. 2009. Seção 1.

BRASIL. Ministério da Integração Nacional. Portaria nº 331, de 7 de agosto de 2009. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, nº 151, p. 30, 10 ago. 2009. Seção 1.

COLOSSI, Cianus Luíz; ARCHANGELO, Flávio Aurélio Braggion; MEDERIOS, Miguel Angelo Conceição. A importância do Radioamadorismo. Disponível em: <https://pt.scribd.com/document/22628297/I mport-an-CIA-Do-Radioamadorismo>. Acesso em: 10 mar. 2020.

CONFEDERAÇÃO NACIONAL DE MUNICÍPIOS – CNM. Defesa Civil e Prevenção de Desastres: Como seu Município pode estar preparado – Coletânea Gestão Pública Municipal: Gestão 2017-2020 – Brasília: CNM, 2016.

IARU. History of IARU. Disponível em: < https://www.iaru.org/about-us/organisation- and-history/history-of-iaru/>. Acesso em: 28 mar. 2020.

JARDIM, Arison. Radioamadores do Acre são convidados a participar de ações de defesa civil. Disponível em:< https://www.iaru.org/about-us/organisation- and-history/history-of-iaru/>. Acesso em: 20 mar. 2020.

MAXIM, Hiram Percy. The Radio Amateur. In CODEL, Martin (Ed.), Radio and Its Future, Harper & Brothers Publishers, New York, 1930. p. 140.

NETO, Mauro Cerri. Aspectos Jurídicos das Atividades de Defesa Civil. Brasília: Secretaria Nacional de Defesa Civil, 2007.

RODRIGUES, Antonio Paiva. Sua Excelência, o Rádio. 1ª Ed. São Paulo: Biblioteca24horas, 2009.

ARTIGO CIENTÍFICO

ÁREA DE CONCENTRAÇÃO

HISTÓRIA MILITAR

A TELEGRAFIA COM FINS MILITARES NO BRASIL E O SEU EMPREGO NAS OPERAÇÕES ESPECIAIS

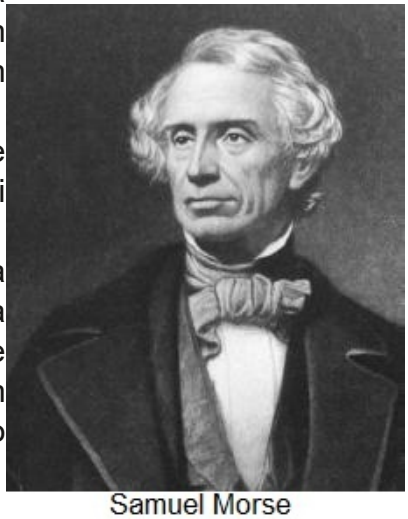
2º SGT ANTONIO AGRÍCOLA LIMA DE OLIVEIRA

RESUMO: Com o advento da internet e da telefo- nia celular, esperava-se que a comunicação por meio de rádio transceptor, entre cidadãos co- muns, caísse em desuso. Mas, não foi o que aconteceu. Tudo isso por conta de que, a co- municação via rádio oferece a oportunidade de se relacionar e formar comunidades com valo- res próprios, como a satisfação de prestar assistência em situações extremas. A função soci- al e a prestação de serviços são algumas das principais virtudes funcionais do radioamador. É, de certa maneira, reconhecido o importante papel desempenhado pelos radioamadores de todo o mundo, principalmente, em situações de emergência e catástrofes. As comunicações de radioamador são das mais confiáveis em circunstancias extremas, em consequência das vulnerabilidades que o sistema de comunica- ções, hoje existente, constitui. Surge no Brasil a Rede Nacional de Emergência de Radioama- dores – RENER, uma importante reserva nacio- nal de comunicações, usada em situações de calamidade, desastre natural, ameaça à vida e à integridade do cidadão, em apoio à Defesa Civil. Através deste artigo, baseado em revi- sões bibliográficas de artigos, livros, periódicos e em legislações nacionais, é possível se apro- ximar mais do serviço prestado pelos radioamadores, com as suas capacidades voluntario- sas de mobilização, de intervenção, e ainda de capacidades técnicas e atuação junto à defesa civil.

Palavras Chaves: COMUNICAÇÕES DE EMERGÊNCIA; DEFESA CIVIL; GERENCIAMENTO DE CRISES; RADIOAMADOR ; RADIOCOMUNICAÇÃO.

1 HISTÓRICO

Samuel Finley Breese Morse nasceu em Charlestown, Massachusetts, em 27 de abril de 1791. Samuel se formou no Yale College em 1810. Ele desejava seguir uma carreira artística, mas seu pai se opôs a isso. Samuel conseguiu um emprego como balconista em uma livraria de Charlestown. Durante esse tempo, ele continuou a pintar. Seu pai reverteu sua decisão e em 1811 permitiu que Morse viajasse para a Inglaterra para se dedicar à arte. Durante esse tempo, Morse trabalhou na Royal Academy com o respeitado artista americano Benjamin West (1738–1820).



Samuel Morse

Em outubro de 1832, Samuel Morse retornou aos Estados Unidos, seu país de origem, após ter vivido durante alguns anos na Europa. Durante a viagem, ele conheceu Charles Thomas Jackson, um excêntrico médico e inventor, com quem discutiu eletromagnetismo. Jackson garantiu a Morse que um impulso elétrico poderia ser conduzido até mesmo por um fio muito longo.

Posteriormente, Morse lembrou que reagiu a essa notícia com o seguinte pensamento: Se assim for, e a presença de eletricidade pode ser tornada visível em qualquer parte desejada do circuito, não vejo razão para que a inteligência não seja transmitida instantaneamente pela eletricidade a qualquer distância. (Samuel Morse).

Imediatamente, ele fez alguns esboços de um dispositivo para cumprir esse propósito. Ainda que lecionasse arte na Universidade da Cidade de Nova York, o telégrafo nunca esteve longe da mente de Morse. Há muito tempo ele se interessava por engenhocas e inclusive já possuía uma patente de uma invenção. Além disso, Morse começou a frequentar palestras

públicas sobre eletricidade.

Seus esboços no ano de 1832 haviam delineado claramente as três partes principais do telégrafo: um remetente, que abre e fecha um circuito elétrico; um receptor, que usa um eletroímã para registrar o sinal; e um código, que traduz o sinal em letras e números.

Em janeiro de 1836, Morse havia confeccionado um modelo funcional do dispositivo o qual apresentou a um amigo. Este, por sua vez, o aconselhou sobre desenvolvimentos recentes no campo do eletromagnetismo, especialmente o trabalho do físico americano Joseph Henry (1797-1878), cientista da matéria e energia. Como resultado, Morse conseguiu melhorar muito a eficiência do seu dispositivo.

Em setembro de 1837, Morse formou uma parceria com Alfred Vail, que contribuiu com dinheiro e habilidade mecânica, e assim solicitaram a patente nos Estados Unidos. Esta permaneceu em dúvida até 1843, quando o Congresso aprovou trinta mil dólares para financiar a construção de uma linha telegráfica experimental entre a capital Washington D.C. e a cidade de Baltimore, em Maryland. Foi nessa linha, em 24 de maio de 1844, que Morse espalhou sua famosa mensagem: "O que Deus fez!" Ele estava disposto a vender todos os seus direitos sobre a invenção ao governo federal por cem mil dólares, mas uma combinação de falta de interesse do Congresso e a ganância da iniciativa privada frustraram o plano.

Ao invés disso, ele passou seus negócios para Amos Kendall. Morse então se estabeleceu para uma vida de riqueza e fama, sendo generoso em suas doações de caridade e foi um dos fundadores do Vassar College, em 1861.

Durante seus últimos anos de vida, no entanto, houve muitos questionamentos sobre o quanto ele havia sido assistido por outras pessoas, especialmente Joseph Henry, na concepção de sua invenção.

Samuel Morse morreu na cidade de Nova York em 2 de abril de 1872.

2 A TELEGRAFIA NO BRASIL

A primeira linha telegráfica do Brasil era subterrânea e possuía 4,3 mil metros de extensão. Construída por determinação do imperador D. Pedro II em 1852, ligava o Palácio Imperial da Quinta da Boa Vista ao Quartel General do Exército no Campo de Sant'Annna, no Rio de Janeiro, capital do império.

Na década seguinte, a deflagração da Guerra do Paraguai acarretou em uma grande expansão das linhas telegráficas no Brasil. Segundo analistas militares, após a derrota na batalha do Curupaiti em 1866, causada principalmente pela inexistência de um sistema de comunicações eficiente, foi desencadeada a construção de redes telegráficas com a finalidade de manter as comunicações entre os campos de batalha e o centro do poder no Rio de Janeiro.

Cabine do Telégrafo no Morro do Castelo

Essa necessidade impôs a construção de uma linha que conectava a Corte à frente de batalha, efetivada pela Repartição Geral dos Telégrafos, onde seu objetivo era diminuir o interstício temporal nas comunicações e possibilitar as tomadas de decisão com mais rapidez e eficácia.

O lançamento dos cabos acompanhava a direção do contingente bélico, inclusive com trechos de linhas lançadas em terras paraguaias. Além disso, foram aproveitadas as linhas já existentes naquele país, conforme as tropas avançavam.

2.1 A FORMAÇÃO DE TELEGRAFISTAS CIVIS E MILITARES

Durante a Segunda Grande Guerra, viu-se a necessidade de empregar a telegrafia em atividades administrativas rotineiras, de comando e controle, assim como em outras mais complexas nos níveis tático, operacional, estratégico e político.

Na década de 1940, foi criada a 1ª

Companhia de Transmissões e depois o Grupo Telegráfico e Telefônico que englobava telegrafistas, teletipistas e mecânicos de material de comunicações. Nesse mesmo período, os quartéis foram equipados com redes telegráficas e telefônicas.

Durante a reforma Capanema de 1942, a telegrafia foi incluída na grade curricular de algumas escolas de ensino médio/técnico, confirmando naquele momento a relevância das comunicações no contexto da segurança nacional.

Embora o Brasil já estivesse preparando telegrafistas há décadas para operarem nas estações rádio, foi somente no ano de 1942 que o Estado passou a investir na formação desses profissionais para o emprego militar, ano em que uma turma de setenta e oito militares concluiu o Curso Especial de Transmissão.

2.2 A INCLUSÃO DA DISCIPLINA TELEGRAFIA NO CURSO DE FORÇAS ESPECIAIS

Em 1957, foi criado o então Curso de Operações Especiais que tinha como base da sua grade curricular as disciplinas dos cursos de “Rangers” e “Special Forces”, ambos do exército norte-americano.

Nós intentávamos ser os melhores em tudo. Depois reconhecemos que não podemos ser em tudo, mas gostávamos de ser os melhores no máximo de atividades. Isso nos inspirou a prosseguir, a estudar, a tentar, a experimentar. A ideia conseguiu adeptos e seguidores. (Cel R1 Paulo Filgueiras Tavares, Operador Especial 02).

Foi a partir dessa mentalidade de autoaperfeiçoamento, tentativas e experimentos, integralmente adaptada à realidade do Exército Brasileiro, que os pioneiros se enveredaram nos caminhos dos “pontos” e “traços” da telegrafia. Não se sabe ao certo quando a telegrafia foi introduzida como assunto no Curso de Operações Especiais, que mais adiante se tornaria o Curso de Forças Especiais, mas estima-se que foi no início dos anos 60.

Na década de 1970, esse meio de comunicação foi utilizado no desenvolvimento das operações no combate à guerrilha urbana e rural que tentou se instalar no Brasil naquela época.

Logo após, no inicio dos anos 1980, os 2 ° Sgt Aguiar e 3 ° Sgt Panichi, realizaram todo o curso de telegrafia na EsCom, naquela época sediada na cidade do Rio de Janeiro, como ouvintes, pois os mesmos não eram da arma de comunicações. Após a conclusão do curso, conseguiram adaptar, difundir e manter o conhecimento nas Forças Especiais.

Na década seguinte, o advento tecnológico dos equipamentos e meios de transmissão e recepção, fez com que o Exército Brasileiro, após estudos prévios, extinguisse o curso de telegrafia em 1999. Concluiu-se na época que essa modalidade de comunicação seria substituída por outras variantes mais modernas, segundo estudos do Estado-Maior do Exército. Alinhado com o EME, o CFEsp retira o assunto Telegrafia da grade curricular dos especialistas em comunicações, permitindo assim a inclusão de novos conhecimentos, adequando as capacidades operativas dos especialistas às realidades de emprego do C² em operações de amplo espectro, nos níveis operacional e estratégico.

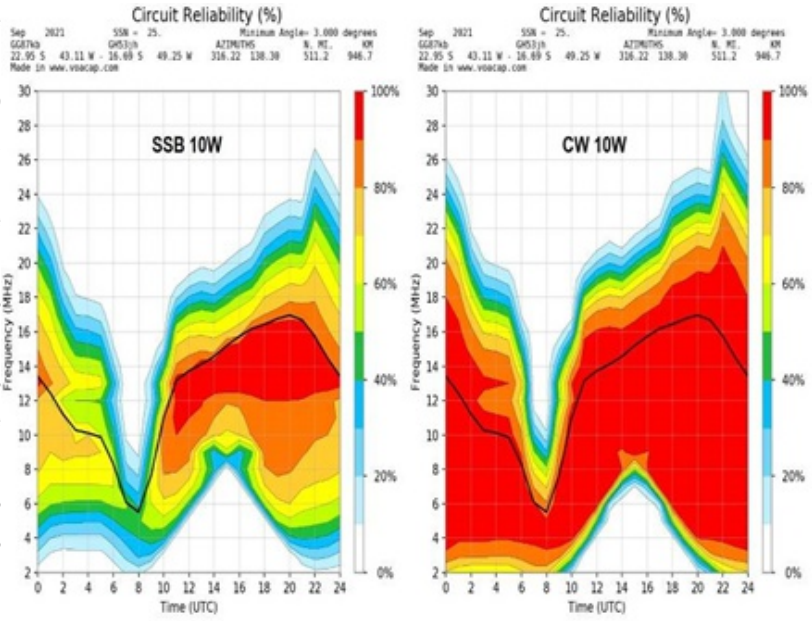
“Após dois anos de suspensão do curso de telegrafia, viu-se a real necessidade de manter essa capacidade...”

Após dois anos de suspensão do curso de telegrafia, viu-se a real necessidade de manter essa capacidade, concomitantemente à informática e suas evoluções tecnológicas. Sendo assim, a Força Terrestre decide reativar esse imprescindível, confiável e seguro meio de comunicação.

Em 2001, o curso retornou com a duração de cinco meses. Dessa maneira, permanece ativo até hoje e funciona nas dependências da Escola de Comunicações, sediada no CComGEx em Brasília-DF. Porém, o mesmo não ocorreu na grade curricular dos especialistas em comunicações do CFEsp. O

assunto somente retornou aos quadros de trabalhos semanais no ano de 2017, através do entusiasta da telegrafia e, na época monitor do CFEsp, o então 2° Sgt Mattozinho, com o apoio do Cap R1 Dias e do St Belchior, ambos do corpo docente da EsCom.

No PCI de 2020, foi possível reunir os meios necessários para a confecção dos adaptadores e manipuladores. Alguns materiais foram adquiridos no comércio local, pois não constam na cadeia logística. Após 10 (dez) dias, os militares do CIOpEsp receberam 4 conjuntos de telegrafia adaptados para o equipamento rádio militar, confeccionados pelo 2 °Sgt Romão.



Predição do Enlace Ionosférico - SSB vs CW (Voacap.com).

As possibilidades do emprego da modulação em CW foram apresentadas aos alunos do Curso de Forças Especiais na EsCom e complementadas na semana de Guerra Eletrônica, no CIGE, durante a fase técnica do curso.

A ideia inicialmente discutida entre os instrutores e alunos do CFEsp era empregar o CW utilizando um código próprio, com a finalidade de obter um maior alcance no enlace HF, pois a telegrafia possui muito pouca informação no sinal, fato que demanda menos potência de transmissão e aumenta consideravelmente a distância e eficácia do enlace. Obviamente, sempre são empregadas mensagens preestabelecidas e Medidas de Proteção Eletrônica – MPE, além disso, o ruído emitido na utilização do CW é mais difícil de sensibilizar os atuais equipamentos de guerra eletrônica.

Pode-se verificar nos gráficos de predição do enlace HF abaixo que a diferença entre as modulações SSB e CW é enorme, sendo este último, o que apresenta maior garantia do enlace, é empregado na telegrafia. Foi utilizado um enlace hipotético entre Niterói-RJ e Goiânia-GO (946,7km) e 10W de potência de transmissão para gerar as predições. A área em vermelho representa 100% de garantia do enlace, de acordo com o horário (UTC) e a frequência (MHz).

A iniciativa de se retomar os conhecimentos no emprego do CW originou-se da experiência dos atuais instrutores especialistas em comunicações do CIOpEsp, após vários anos cumprindo missões reais, onde puderam vivenciar os empecilhos de se estabelecer um enlace HF. Essa dificuldade se faz mais perceptível na região amazônica, onde as principais capacidades de softwares e hardwares dos meios de comunicações modernos geralmente não conseguem romper as intempéries e o isolamento geográfico daquele ambiente operacional.

Essa tecnologia, relativamente antiga, acabou mostrando-se uma ferramenta de inestimável valor para os Operadores de Forças Especiais recém-formados planejarem missões futuras, com a experiência adquirida durante o curso, aumentando a capacidade operacional dos DOFEsp.

Atualmente, a telegrafia encontra-se consolidada na formação dos OpFEsp e é largamente utilizada nas operações militares (situações integradoras) desencadeadas pelas frações operacionais do CFEsp.

3 A REDE RÁDIO DO SISTEMA DE COMUNICAÇÕES DO EXÉRCITO BRASILEIRO – RRF/EB

A Rede Rádio do Sistema de Comunicações do Exército divide-se em RRF Principal (RRFP) e Secundária (RRFS). A RRFP é composta por todos os CTA/CT e a RRFS pelo CTA/CT e suas estações subordinadas.

Há 07 (sete) Centros de Telemática de Área, vinculados aos comandos militares de área e 05 (cinco) Centros de Telemática, vinculados às regiões militares isoladas, com 159 (cento e cinquenta e nove) estações rádio conectadas.

Dessa forma, todos os quartéis estão apoiados diretamente pelo serviço de radiotelegrafia que conta com 444 (quatrocentos e quarenta e quatro) militares

Aluno do CFEsp - Esp Com, Utz manipulador CW.

da ativa habilitados a operar o sistema em Código Morse e transmissão de dados. Destes militares habilitados, excluem-se os operadores de forças especiais, embora possuam as capacidades técnicas, não apresentam a certificação funcional.

O projeto atingirá a todos os segmentos do Exército Brasileiro que apoiam ou são apoiados por unidades operacionais do COpEsp, considerando o amplo emprego dos meios de comunicações nas OM e redes de C2 em operações.

REFERÊNCIAS

Samuel F. B. Morse Biography. Encyclopedia of World Biography. 2009. Disponível em: <https://www.notablebiographies.com/Mo-Ni/Morse-Samuel-F-B.html>. Acesso em: 02 Set 2021.

BRASIL. Há 168 anos, era inaugurada a primeira linha de telégrafo do Brasil. Biblioteca Nacional. 2020. Disponível em: <https://www.bn.gov.br/acontece/noticias/2020/05/ha-168-anos-era-inaugurada-primeira-linha-telegrafo>. Acesso em: 10 Set 2021.