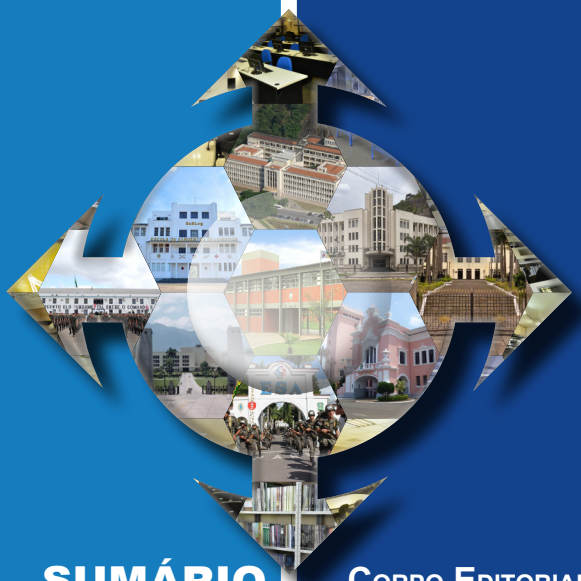
ISSN 2594-3952



O Comunicante

SUMÁRIO

Revista Científica da Escola de Comunicações

Escola Coronel Hygino Corsetti

VOLUME 10 - Nº 1

Junho 2020

ISSN 2594-3952

O Comunicante

SUMÁRIO

Revista Científica da Escola de Comunicações

Escola Coronel Hygino Corsetti

VOLUME 10 - Nº 1

Junho 2020

O COMUNICANTE
Revista Científica da Escola de Comunicações

Ano 10 - Nº 1

Junho 2020

ISSN 1968-6029

ISSN 2594-3952 (Digital)

Escola de Comunicações - EsCom

Escola Coronel Hygino Corsetti

EDITORIAL

A presente edição da Revista “O Comunicante” apresenta uma seleção de artigos produzidos pelo corpo docente e discente da Escola, além de colaboradores externos, nas Áreas de Defesa Nacional, com enfoque em Comunicações Militares, Ciência e Tecnologia.

Pode-se observar, nesta publicação, o desenvolvimento de novas tecnologias que contribuem para a evolução das telecomunicações, ameaças cibernéticas frequentemente enfrentadas pelo Exército Brasileiro, os ativos de rede normalmente infectados, alvos mais compensadores e formas de proteção. Os temas são abordados em textos de fácil leitura, contribuindo para a atualização dos conhecimentos técnicos dos leitores que lidam com o desafio de prover o apoio de comunicações.

Desta forma, a EsCom, que completará neste ano 99 anos de existência, mantém a sua missão, contribuindo para informar e ampliar o debate em torno de temas de caráter técnico doutrinário, preservando as tradições desta casa, na difusão de assuntos relacionados ao exercício do Comando e Controle.

O Comando da Escola de Comunicações 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.

SANDRO SILVA CORDEIRO - Cel
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 semestral (junho e dezembro) e se reserva ao direito de realizar edições especiais, além das previstas.

O Comunicante - Revista Científica da Escola de Comunicações - Volume 10, Nº 1 (Jun/2020)
Brasília-DF: Escola de Comunicações. 2020 48p; 29,7 cm X 21,0 cm

Publicação Semestral
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

CIBERNÉTICA

PROTEÇÃO CONTRA ATAQUES DE PHISHING NO EXÉRCITO BRASILEIRO

Daniel Moura Félix Cardoso[1], Daniel Bomfim Nunes[2]

Pós-graduado em Operações Militares[1], Técnico em Eletrônica, Especialista em Manutenção de Comunicações[2]

Resumo: Este trabalho apresenta um estudo acerca do mais comum ataque sofrido diariamente por pessoas, em esferas do poder público e na iniciativa privada, o Ataque de Engenharia Social, Phishing. Foram estudadas algumas formas que são utilizadas normalmente nesse tipo de ataque, quais ativos de rede normalmente podem ser infectados e quais os alvos mais compensadores. Foi identificado também o ataque de Spear Phishing como ferramenta direcionada de ataque e apresentadas medidas de proteção contra esse tipo de ataque. A intenção desse artigo foi a de conscientizar o público militar da ameaça existente no Ambiente Cibernético e que qualquer um pode estar suscetível a sofrer esse ataque.

Palavras-chave: Engenharia Social. *Phishing*. Ataque. Ambiente Cibernético. Exército Brasileiro

INTRODUÇÃO

Com o crescimento exponencial da utilização de dispositivos informacionais por militares do Exército Brasileiro (EB), sejam ativos particulares ou material da própria Unidade Militar, pôde-se observar o aumento do número de casos de tentativas de invasão das redes militares pelos mais diversos tipos de ataque. Dessa forma, os diversos Centros de Telemática (CT) que se encarregam de prover e manutenir a rede lógica do Exército garantem uma certa segurança efetiva desses links com a Internet e Intranet do EB.

Partindo do princípio que praticamente todos os militares utilizam da conexão com a Internet para trabalhar, pesquisar, ensinar e nas horas vagas para o lazer, coube incrementar mais ainda essa segurança ofertada pelos CT nas próprias Unidades, pelo estabelecimento de Políticas de Segurança da Informação e Comunicações (POSIC), segregação de rede corporativa das utilizadas para interesses particulares (geralmente dispositivos particulares não acessam a rede corporativa), implementação de dispositivos como Firewall, IPS/IDP, estabelecimento de Proxy, monitoramento da Rede e outros procedimentos.

Podemos fazer um paralelo de uma rede lógica com uma corrente. Esta é formada por diversos elos. Esses elos são forjados individualmente e possuem em sua liga metálica diferentes composições (até mesmo pela mistura metálica e temperatura de forja do metal). A corrente é tão forte quanto o elo mais fraco de sua corrente. Da mesma forma, qualquer ativo da rede pode ser entendido como um elo. Cada um deles é responsável pela manutenção do acesso à rede.

Mas se mesmo com todas essas formas de segurança pudesse ser elencada uma forma de invasão mais simples? E se no final de tudo, mesmo com todo esse nível de segurança implementado pelos melhores gerentes de rede e gerentes de segurança das respectivas Unidades, o mais simples dos ataques fosse realmente efetivo? Onde pode-se encontrar esse tal de “elo mais fraco”? Historicamente a maioria dos programadores, gerentes de rede e de segurança, e outros conhecedores da área de Tecnologia da Informação (TI) apontam o mesmo como sendo elo o mais fraco: o usuário.

O usuário é a razão de ser de qualquer rede informacional pautada em dispositivos lógicos. Também conhecido como “Cliente”, usufrui dos dispositivos, visando um produto final nem sempre ligado à Computação propriamente dita. Até mesmo porque a TI normalmente é uma atividade “meio” para toda a máquina empresarial ou particular.

O grande problema é que o usuário nem sempre tem o devido conhecimento (ou paciência de estudar e aprender) sobre segurança da informação. Normalmente quer apenas comprar ou receber a máquina e usar sem aprender sobre as ferramentas que ela tem ou sobre suas capacidades. Aí que está o problema. O usuário sempre prefere ter mais usabilidade que é a facilidade com a qual um equipamento ou programa pode ser usado, em detrimento da segurança do seu ativo, muitas das vezes permitindo que atualizações de segurança deixem de ser instaladas nos seus computadores.

Como exemplo disso, segundo Cossetti (2017), o ransomware Wannacry, que explorou uma vulnerabilidade nos Sistemas Operacionais (SO) Windows 7, Windows 8, Windows Server 2008 e outras versões da empresa Microsoft, já tinha sido corrigida 2 meses antes, mas muitos usuários simplesmente deixaram as atualizações do seu SO no modo manual e não as fizeram antes do ataque.

Com o crescente número de reportagens veiculadas na mídia (inclusive mídias sociais) tratando sobre quebras de segurança, mais usuários estão começando a aceitar opiniões de especialistas da área de Segurança da Informação para implementar medidas de segurança ativas e passivas nos seus dispositivos e melhoria nos seus procedimentos diários de utilização de computadores, tablets e smartphones.

Esses ataques orientados aos usuários e que nem sempre utilizam diretamente dispositivos informacionais são conhecidos como Engenharia Social. Nesse nicho, existem diversas formas de ataque que podem ser empregados. Será analisado neste artigo o ataque de Phishing, quais danos ele pode trazer à rede corporativa e quais as formas de combater a ocorrência desse ataque no Exército Brasileiro.

1 DESENVOLVIMENTO

Segundo a Cartilha de Segurança para Internet Cert.Br (2020), os ataques costumam ocorrer na Internet com diversos objetivos, visando diferentes alvos e usando variadas técnicas. As motivações que levam *Hackers Black Hat, Crackers* ou Engenheiros Sociais a realizarem ataques são os mais variados, sendo os abaixo relacionados como mais importantes já elencados pela comunidade internacional da área de Segurança da Informação (SI):

a. Demonstração de poder: mostrar a um órgão público, corporação ou empresa que pode ser invadido ou ter serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente;

b. Prestígio: vangloriar-se, perante outros atacantes ou sobre a própria comunidade da Internet, por ter invadido computadores, tornar serviços inacessíveis ou desfigurar sites visados (*Defacement*); disputar com outros atacantes para verificar quem realiza o maior número de ataques ou ser o primeiro a conseguir atingir um alvo específico;

c. Motivações financeiras: coletar e

utilizar informações confidenciais de usuários para aplicar golpes;

d. Motivações ideológicas: tornar inacessível ou invadir sites para negar o seu serviço ou mudar ideias que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia; e

e. Motivações comerciais: inviabilizar o acesso ou invadir sites e dispositivos de empresas concorrentes, buscando impedir o acesso dos clientes ou comprometer as suas reputações.

Pode-se imaginar que estes ataques nem sempre consigam atingir objetivos por completo pela forma como são desferidos e o seu dano causado aos alvos, mas os realizados com maior probabilidade de êxito são aqueles que envolvem diversas técnicas de ataque e normalmente se iniciam com técnicas de Engenharia Social.

Alguns autores quando discorrem sobre os alvos, apontam que existe uma escala de estados de percepção do alvo em relação ao ataque/exploração. Parece curioso e até um pouco absurdo tentar elencar uma “escala de estados de percepção do alvo”, mas observando com profundidade, o estado em que se encontra o atacado pode influir diretamente no êxito do ataque e da sua própria continuidade.

Pode-se elencar como estado inicial aquele em que o alvo sabe que está sendo atacado/explorado e sabe quem é o autor. Essa é a situação mais favorável para o alvo, pois irá aumentar o máximo possível o seu nível de segurança direcionando para a forma de ataque que sabe ou acredita que será empregada contra ele (ou pelo menos de quem está vindo o ataque). No segundo estado, o alvo sabe que está sendo atacado/explorado mas não sabe quem é o autor. Dessa forma, o alvo precisa buscar incrementar ao máximo a sua segurança em todas as frentes.

Um terceiro estado é aquele que o alvo não sabe que está sendo atacado/explorado e não sabe quem é o autor. Dessa forma, tudo ocorre normalmente na vida do alvo e o atacante permanece explorando a vulnerabilidade enquanto esta não for eliminada. O estado mais favorável ao atacante é aquele em que o alvo não sabe que está sendo atacado/explorado, porém garante que não está sendo alvo de ataques e explorações. Essa atitude tomada por um gerente de segurança em sua rede é muito nociva pois pode tranquilizar os usuários acerca de uma situação inverídica e pode causar danos irreversíveis ao seu órgão ou empresa.

1.1 ENGENHARIA SOCIAL

Ao pensar no fator segurança da informação/cibernética é necessário elencar primeiramente todos os aspectos tecnológicos possíveis, sejam eles dispositivos, aplicações ou sistemas que venham a prover a segurança planejada. Desta feita, todo o projeto de segurança física e lógica é elaborado e aperfeiçoado continuamente a fim de mitigar as ameaças existentes no cenário cibernético. No entanto, um fator primordial, muitas vezes esquecido, é o sujeito que opera, controla, acessa, manipula e realiza as mais variadas tarefas através dos equipamentos e sistemas aos quais possuem acesso.

E por que o fator humano é tão vulnerável? Isto ocorre devido à individualidade reservada a cada um, ou seja, para cada indivíduo há interesses pessoais diferentes, os quais culminam em rotinas de trabalho diferenciadas e conceitos diversificados sobre o que é seguro ou não. Esta falta de informação, capacitação ou mesmo interesse quanto ao que convém para garantir a segurança de dados é o que torna os recursos humanos tão susceptíveis a quebras ou falhas de segurança, quer sejam intencionais ou não. Dessa forma o fator humano torna-se um alvo de grande valia para os Engenheiros Sociais.

A Engenharia Social é uma técnica (ou conjunto de técnicas) por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. É considerada uma

prática de má-fé, usada por fraudadores para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de angariar ganhos financeiros, aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O popularmente conhecido "conto do vigário" utiliza Engenharia Social (CERT.BR, 2020).

A segurança cibernética se baseia em quatro pilares, os quais são confidencialidade, disponibilidade, integridade e autenticidade da informação. Segundo Jeremy *et al* (2015):

> A Engenharia Social, no contexto da Segurança da Informação é a manipulação de pessoas para levá-las inconscientemente a executar ações que causam danos à confidencialidade, integridade e disponibilidade de recursos da organização, incluindo a informação, os sistemas de informação e os sistemas financeiros (*apud* MAULAIS, 2016, p. 23).

Um engenheiro social em alguns casos, costuma estudar as preferências, acessos, páginas visitadas, ambiente social, amizades, objetos pessoais, opiniões políticas e tudo aquilo que possa ajudar a traçar um perfil do alvo desejado. Com menos riqueza de detalhes, há também, o estudo de grupos com características comuns, por exemplo "pessoas com dívidas" e "pessoas que precisam de emprego".

Com o estudo mais pormenorizado é comum o atacante coletar informações nas redes sociais. Isso ocorre porque, sem uma consciência de segurança da informação, as pessoas acabam publicando, registrando, arquivando na rede e compartilhando informações pessoais e, em alguns casos, até mesmo confidenciais. Então, o engenheiro social analisará os dados que lhe forem convenientes e, a partir daí, formulará uma "porta de entrada" para acessar a informação que o alvo estudado pode fornecer. O ideal, para o atacante, é que a obtenção do que deseja ocorra de modo que a vítima não perceba e para isso há diversas formas.

O Engenheiro Social pode se aproximar de maneira mais rápida, como uma falsa entrevista de emprego, onde retirará o máximo de informações aproveitando a vulnerabilidade de um sujeito que deseja trocar de emprego, por exemplo. Mas também pode ser um processo mais demorado onde espera que a vítima se sinta confortável o suficiente para compartilhar informações sem perceber sua importância. Uma ameaça em troca de informação pode ocorrer quando inocentemente publicamos ou registramos em redes sociais conteúdos como composição familiar, horários da rotina pessoal, local e função em que determinada pessoa trabalha.

No caso em que grupos com características comuns são tidos como alvo, o método de ataque é mais abrangente. Uma ligação com a intenção de oferecer um empréstimo mediante um cadastro e que pergunta sobre dados pessoais é um caso corriqueiro onde o objetivo é apenas coletar documentos pessoais e financeiros. Todas essas informações são passadas pela própria vítima por confiar em quem está do outro lado da linha.

Com a diária utilização de dispositivos que acessam a Internet, as pessoas costumam trocar informações ou realizar cadastros através de seus e-mail pessoais e, no caso de algumas organizações, dos e-mails funcionais (e-mails corporativos utilizados normalmente para assuntos que dizem respeito ao trabalho).

No caso do Exército Brasileiro, por exemplo, uma ligação ou e-mail contendo diretrizes ou solicitando dados e que se caracterize como uma autoridade tem maiores chances de ser seguido. Isso ocorre pois o Engenheiro Social sabe que os militares seguem o princípio da hierarquia e no caso do público menos experiente a tendência é não agir com a mentalidade da segurança da informação.

As mensagens de e-mail podem conter links que direcionam a vítima para um site falso que coleta informações ou mesmo que realiza o download de alguma ferramenta com um malware (software malicioso) escondido. Além disso, há a possibilidade de ameaças

via e-mail. Todas essas modalidades se enquadram numa forma de ataque denominada *Phishing*.

1.2 *PHISHING*

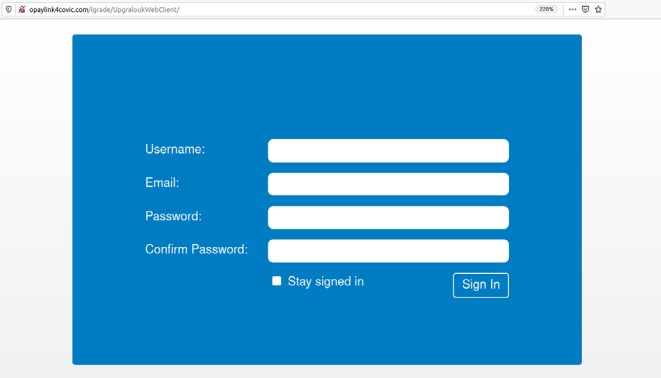
O *Phishing-Scam, Phishing/Scam* ou simplesmente *Phishing* é o tipo de golpe por meio do qual um atacante tenta obter dados pessoais e financeiros de um usuário, de maneira fraudulenta, pela utilização combinada de meios técnicos e Engenharia Social (CERT.BR, 2020). Dentro daquela ideia de que o usuário é o elo mais fraco da corrente por necessitar do serviço e desconhecer muito da Computação, é mais exitoso tentar ludibriá-lo com técnicas nem sempre “ortodoxas”.

O *Phishing* ocorre por meio de envio de mensagens eletrônicas (normalmente por e-mail) que tentam coagir, convencer ou enganar o alvo de algo que deva ser feito. No caso da coação, geralmente o alvo é colocado em uma situação que deva cumprir com tarefas para poder impedir um mal maior. Recentemente, um e-mail foi encaminhado para uma determinada Unidade Militar que requeria que fossem adquiridos cartões de crédito pré-pagos e enviadas fotos dos cartões para um específico e-mail, pois o dito Hacker informou que havia acessado à máquina e criptografaria o seu armazenamento inteiro. O mesmo atacante informou que tinha informações sigilosas de cunho pessoal e que iria expor o alvo se não fossem cumpridos os procedimentos.

Já a tentativa de convencimento é aquela que o alvo recebe informações que procuram atrair a sua atenção, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira. Pelo convencimento, o alvo pode fornecer informações, recursos financeiros ou dados pessoais ao atacante, clicando em algum link ou literalmente enviando informações para o atacante, por meio de e-mail ou de uma página de que receba os dados.

Enganar o alvo envolve tentar se passar por comunicação oficial de uma instituição conhecida, como um banco, empresa ou site popular. Basicamente esse tipo de ataque é mais efetivo com aquele tipo de usuário que realiza muitas transações financeiras pela Internet. Comumente, são utilizadas páginas falsas clonadas das reais; de instalação de códigos maliciosos de toda ordem, projetados para coletar informações sensíveis; ou de preenchimento de formulários contidos na mensagem ou em páginas Web. Em maio de 2020, foi veiculada nas contas do EBMail de vários militares do Exército uma mensagem dizendo que o militar deveria atualizar os dados de usuário, e-mail e senha para que não fosse desativada permanentemente sua conta de e-mail.

Figura 1 Tela de login falsificada



Fonte: O Autor (2020)

O que é muito claro nesses ataques de Phishing é a urgência em que o alvo é colocado, necessitando sempre fazer tudo de forma rápida para que “o pior não ocorra”. Essa urgência tem a finalidade de evitar que a vítima tenha tempo para raciocinar melhor e evitar o golpe. Alguns outros ataques são direcionados apontando uma solução aparentemente plausível para o problema apresentado, como por exemplo o ataque que diz que o antivírus da vítima não está atualizado mas um link apresentado em um e-mail pode resolver esse problema. Analisando friamente a situação, dificilmente um e-mail recebido estaria orientado exatamente ao antivírus de uma máquina específica.

Ainda assim, nos e-mails de *Phishing*, o atacante nem sempre dispõe de informações específicas para o seu alvo. As poucas infor-

mações apresentadas no ataque são genéricas, não direcionadas. Dessa forma, o *Phishing* pode ser distribuído para muitos alvos, visando atingir o máximo possível de pessoas para poder obter maior resultado, ou pelo menos um alvo para acessar a rede em que aquele usuário está participando.

Segundo o site *Intuit Online Security Center* (2020), as variantes do *Phishing* são o *Vishing, Smishing e Pharming*. Todas essas formas de ataque, baseado no *Phishing* possuem resultado semelhante. O *Vishing* nada mais é do que a mesma técnica de Engenharia Social empregando uma ligação Telefônica e o Smishing por mensagem de texto (SMS ou aplicativos de mensagens). Novamente, assim como o *Phishing*, a ligação telefônica *Vishing* e a mensagem de *Smishing* geralmente requisitam atenção imediata. Já o *Pharming* é um golpe em que o Engenheiro Social instala, utilizando normalmente um link compartilhado por ele, em que este código redireciona todos os cliques feitos em um site para outro site falso sem o consentimento do usuário. Essa tarefa é realizada pela corrupção de direcionamento do *Domain Name System* (DNS), que é responsável em linhas gerais por apontar o endereço lógico, traduzido do endereço escrito na barra dos navegadores. (Site Netspeed, 2019).

Existe ainda uma forma mais específica do *Phishing* chamado de *Spear Phishing.* Essa técnica de Engenharia Social será abordada no capítulo seguinte, visando identificar melhor a sua forma de atuação e porque acaba sendo mais efetiva do que um *Phishing* comum.

1.3 SPEAR PHISHING

O *Spear Phishing* é um tipo de técnica de Phishing que consiste em um ataque direcionado para um alvo específico. Este trabalho normalmente é muito bem feito para que possa cobrir todas as falhas de um ataque de *Phishing*. Na verdade, o *Spear Phishing* normalmente é uma das últimas fases do ataque propriamente dito. Existe uma gama de outras técnicas de coleta de informações que são necessárias a serem realizadas anteriormente para poder enfim aplicar o golpe.

Existem várias maneiras pelas quais um Engenheiro Social pode tentar obter informações confidenciais, tais como:

a. *Dumpster Diving*. Procurar informações nos lixos das empresas;

b. Monitoramento de Rede. Invadir a rede e monitorar o tráfego que ocorre nela ou o tráfego que sai da rede para a Internet;

c. *Open Source Inteligence*. Coletar informações em fontes abertas, como redes sociais ou buscadores da Internet;

d. *Shouder Surfing.* Coletar informações por “cima do ombro” de um alvo*;* e

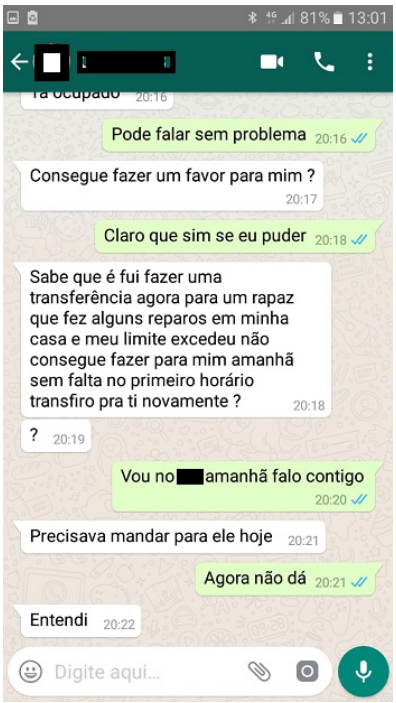
e. *Tailgating*. Acessar setores da empresa impedidos, simplesmente seguindo pessoas credenciadas.

Essas técnicas são apenas algumas das quais podem ser utilizadas para coletar inicialmente informações que subsidiam o ataque de *Spear Phishing* propriamente dito. No próximo passo do ataque, o alvo recebe um contato (e-mail, SMS, telefônico ou outro) em que dados particulares e de conhecimento exclusivo do alvo ou de um círculo de pessoas bastante restrito são apontados inicialmente. Nesse ponto, o Engenheiro Social apresenta o ataque conforme descrito anteriormente, tentando coagir, convencer ou enganar o alvo de que algo deva ser feito.

Na coação, normalmente uma informação ou dados do alvo são apresentados e o mesmo tem pouco tempo para realizar um pagamento ou tomar uma atitude em favor do atacante. Quando a forma é o convencimento ou enganação do alvo, normalmente as informações coletadas anteriormente são utilizadas para dar crédito ao atacante e se fazer passar como uma pessoa/empresa legítima. Acreditando no atacante, o alvo realiza transações financeiras ou a ação desejada em favor desse.

Na Internet, há vários casos de ataques direcionados, em que, após o roubo da conta do aplicativo WhatsApp de um usuário, o atacante realiza contato com um amigo ou parente do titular real do aplicativo (alvo) solicitando transferir dinheiro para uma conta ou pagar um boleto por exemplo.

Figura 2 Conversas Telefônicas

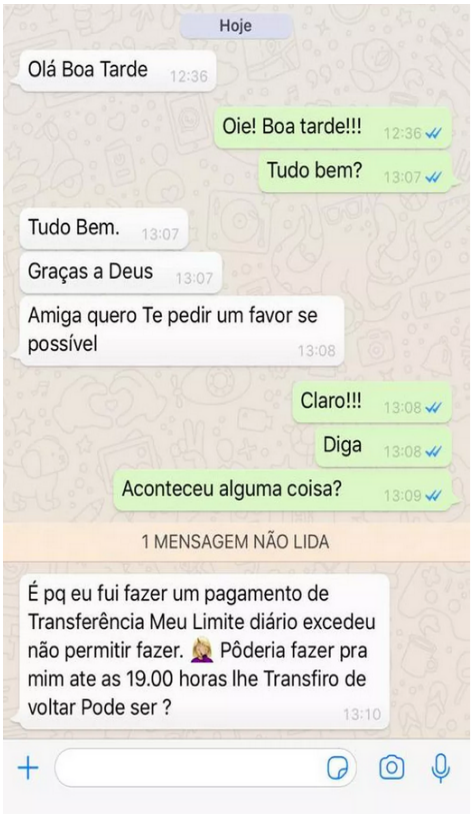


Fonte: Brasil Agora (2019)

Uma história no mínimo curiosa que aconteceu de *Spear Phishing* foi a da venda do jogador de futebol Leandro Paredes, transferido do time russo *Zenit* para o francês *Paris Saint-Germain* (PSG) pelo valor de 40 milhões de Euros.

> Quem ficou feliz com a notícia foi o argentino Boca Juniors: como clube formador do atleta, segundo regras da FIFA, ele tinha direito de receber cerca de 3,5% da venda. (...)
>
> O valor total que o Boca Juniors deveria receber é de € 1,3 milhão. Como o valor é alto, o PSG combinou que pagaria em três parcelas, sendo que a primeira a ser paga cairia dia 6 de março de 2019 no valor de € 519.750,99. (...)
>
> Após checar recibos de comprovação de transferência e algumas semanas passadas, o clube argentino notou que algo deveria ter dado errado. Durante investigação nos documentos e mensagens trocadas entre os times, o Boca descobriu que o dinheiro do PSG foi transferido primeiro para uma conta bancária de uma empresa mexicana, Vector Casa de Bolsa, e depois para um banco em New York, antes de retornar ao México, para uma conta da empresa OM IT Solutions S.A. de C.V. Uma movimentação atípica.
>
> O que aconteceu: cibercriminosos fizeram um esquema de *Phishing* para enganar o PSG. Eles enviaram emails de endereços falsos, parecidos com o domínio real do Boca, com instruções de depósito dos € 520 mil. A diferença entre o email real e o falso estava em apenas 1 caractere. (Site Terra, 2019)

Figura 3 Conversas Telefônicas



Fonte: G1 (2019)

Spear Phishing normalmente é direcionado a grandes empresas, na pessoa de *CEO* (Chefe Executivo), Vice-Presidentes ou Gerentes (principalmente os financeiros), visando anular terceiros que possam assessorar o chefe que se trata de um golpe. No caso apresentado anteriormente, o trabalho de levantamento de dados foi muito bem feito por parte

da equipe atacante, que sabia exatamente o valor, a data e as credenciais de e-mail que entraria em contato com o time PSG para a transação. Faltou por parte do time que depositou o dinheiro verificar exatamente se aquele contato realmente se tratava da parte da empresa que realmente deveria ser paga (Time Boca Juniors).

1.4 PROTEÇÃO CONTRA *PHISHING*

Ao se tratar de Segurança da Informação, é fundamental especificar as Políticas de Segurança da Informação e Comunicação. Estas devem conter, além das especificações técnicas (segurança física e lógica) de proteção, um programa que vise a defesa/proteção contra-ataques de Engenharia Social. Para tal, é essencial que sejam implementadas medidas que promovam uma cultura de segurança bem como a conscientização quanto à vulnerabilidade que todos os usuários podem trazer. Segundo LONG (2013), "A educação é naturalmente considerada um dos principais métodos para se defender contra *Phishing*" (*apud* MAULAIS, 2016, p. 52).

No âmbito de Exército Brasileiro o ideal é que ocorram palestras geridas pelos militares responsáveis pela área de Tecnologia da Informação e Comunicação e aqueles que gerenciam as Agências de Inteligência. As orientações devem ser conduzidas de modo a conscientizar cada usuário de que ele é alvo de ameaças e que possui a responsabilidade quanto à informação que é divulgada. Para tal, é necessário explicar o que é *Phishing*, suas variantes e dar exemplos práticos. Além das palestras, é recomendado que existam cartazes de conscientização e também que informem casos recentes de ataques, e as medidas adotadas para evitá-los. Orientações na páginas da Intranet das Organizações Militares (OM) também são um ótimo recurso para gerar a cultura de segurança.

A partir do momento que os usuários estejam familiarizados com as possibilidades de Phishing é ideal focar no reconhecimento e formas de evitá-lo. As principais recomendações são:

a. Verificar a origem (remetente) das mensagens recebidas;

b. Prender e identificar um documento oficial. Isto se dá observando a confiabilidade da fonte, procurando erros ortográficos, confirmando com outros integrantes da Organização a origem do documento, suspeitando de mensagens contendo links ou solicitando confirmação de dados pessoais;

c. Suspeitar de mensagens que contenham ameaças; e

d. Não fazer download de anexos que estejam em e-mails suspeitos.

O militar que identificar qualquer uma das possibilidades citadas deve imediatamente comunicar o fato ao chefe da Seção de Inteligência e à equipe de Segurança da Informação.

Os gestores da Segurança da Informação na OM que sofreu a tentativa de ataque devem realizar a análise da mensagem enviada bem como dos possíveis danos que ela possa ter ocasionado. Caso a mensagem tenha sido detectada antes de coletar dados, o primeiro passo é fazer a exclusão segura desta e em seguida veicular em todos os canais de comunicação o ocorrido para outros integrantes da rede. Dessa forma, é possível minimizar futuros danos do mesmo ataque. Para o caso em que dados já tenham sido coletados, será necessário fazer uma averiguação da rede e verificar o possível isolamento dos dispositivos e dados que tenham sido infectados ou exfiltrados. Além disso é fortemente recomendada a solicitação de apoio dos Centros de Telemática a fim de mitigar a propagação da ameaça.

CONCLUSÃO

Engenharia Social é uma das maiores armas de um hacker. Nem sempre é necessário ligar um computador para realizar um ataque cibernético. Um hacker de respeito é

aquele que consegue mesclar diversas técnicas de reconhecimento, exploração e ataque para conseguir lograr êxito em sua tarefa. O dever do gestor de Segurança da Informação é garantir que não somente seus servidores, bem como seus dispositivos finais e estrutura lógica, mas também (e muitas das vezes mais importante) os seus usuários estejam preparados para confrontar ataques cibernéticos, direcionados ou não.

Nas palavras do autor do Best Seller A Arte de Enganar e antigo Engenheiro Social Kevin Mitnick:

> Há um ditado popular que diz que um computador seguro é aquele que está desligado. Isso é inteligente, mas é falso: O hacker convencerá alguém a entrar no escritório e ligar aquele computador. Tudo é uma questão de tempo, paciência, personalidade e persistência. Kevin David Mitnick

Muitos presidentes de empresa, chefes de órgãos ou repartições públicas em todos os níveis acabam se atentando para a necessidade da segurança da sua estrutura lógica apenas quando é tarde demais. Um ataque cibernético pode atrasar em anos, talvez décadas de trabalhos realizados. Dificilmente alguma empresa utiliza um sistema que não seja pautado em dispositivos informacionais. Pelo menos não uma que queira trabalhar com velocidade na sua troca de Informação.

Portanto, treinar o Soldado do Exército Brasileiro em cibersegurança é fundamental para manter a segurança da informação da rede corporativa, dos seus ativos de rede, principalmente das informações sigilosas da Força Terrestre. A palavra-chave é conscientização!

Treinamentos periódicos de cibersegurança, alertas quanto aos ataques sofridos na Internet por outros órgãos públicos e empresas particulares, e vigilância contínua da rede são alguns dos procedimentos indicados para se manter uma relativa segurança à Rede. Isso porque não há firewall que impeça um ser humano de ser vítima de um golpe de Engenharia Social! Segundo o Site Proof (2020), essas são algumas medidas fundamentais:

a. Usar senhas fortes: que possuam letras maiúsculas e minúsculas, números, e caracteres especiais. Essas senhas demoram mais para serem quebradas por programas e algoritmos. O Site Kaspersky desenvolveu uma calculadora que apresenta em quanto tempo a sua senha pode ser quebrada. Essa calculadora é está disponível no site *Secure Password Check*, cujo endereço eletrônico é <https://password.kaspersky.com>.

b. Alterar as senhas com frequência;

c. Não usar a mesma senha para mais de um aplicativo, sistema ou website: para cada login, deve ser planejada uma senha distinta da outra, pois senhas variadas impedem a exposição de todas as suas contas se uma delas vazar (também não é muito indicado guardar as suas senhas na própria rede, pois se ela for invadida, todos os logins e senhas serão expostos);

d. Utilizar um gerenciador de senhas: para administrar senhas fortes e variadas sem precisar decorá-las, é interessante utilizar uma ferramenta dessas, de modo que o usuário possa gerar novas senhas aleatoriamente (que não possuam nenhum significado para o usuário e reduzam a possibilidade de serem adivinhadas por Engenharia Social); também pode ser utilizado para compartilhar informações de login com segurança e privacidade com outros usuários;

e. Não clicar em links suspeitos: analisar a URL disponível e no caso de hiperlink, ao passar o cursor do mouse em cima, esse estará disponível. URLs encurtadas (bit.ly), por exemplo, são amplamente utilizadas nas fraudes; e

f. Não abrir anexos não solicitados: podem possuir malwares ou documentação falsa, como um boleto fraudulento.

Quão seguro é a sua senha? A figura 4, produzida por Mike Halsey, do Site Ghacks.net (2012) que aponta quanto tempo leva apro-

ximadamente para serem quebradas as senhas em cada um dos casos de mescla ou não de números, letras maiúsculas e minúsculas e caracteres especiais.

Figura 4 Tempo de quebra das senhas

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Fonte: HALSEY, Mike. 2012.

Apesar do *Phishing* ser amplamente difundido por diversos meios de comunicação, tanto na vida particular quanto na profissional, muitas pessoas continuam sendo alvos exitosos de ataques de Engenharia Social, gerando grande prejuízo financeiro ou informacional. Isso mostra o despreparo que ainda reina entre os usuários que não permanecem alertas aos indícios do ataque tendo consequências desastrosas. Por isso é imperiosa a manutenção dos treinamentos, capacitações e conscientização de todos que participam das redes militares, nem que seja pelo menos por um instante.

PROTECTION AGAINST PHISHING ATTACKS IN THE BRAZILIAN ARMY

ABSTRACT. THIS PAPER PRESENTS A STUDY ABOUT THE MOST COMMON ATTACK SUFFERED DAILY BY PEOPLE, IN SPHERES OF PUBLIC POWER AND IN THE PRIVATE SECTOR, THE ATTACK OF SOCIAL ENGINEERING, PHISHING. SOME WAYS THAT ARE NORMALLY USED IN THIS TYPE OF ATTACK HAVE BEEN STUDIED, WHICH NETWORK ASSETS CAN USUALLY BE INFECTED AND WHICH ARE THE MOST REWARDING TARGETS. THE SPEAR PHISHING ATTACK WAS ALSO IDENTIFIED AS A TARGETED ATTACK TOOL AND PROTECTION MEASURES AGAINST THIS TYPE OF ATTACK WERE PRESENTED. THE INTENTION OF THIS ARTICLE WAS TO MAKE THE MILITARY PUBLIC AWARE OF THE THREAT THAT EXISTS IN THE CYBER ENVIRONMENT AND THAT ANYONE CAN BE SUSCEPTIBLE TO SUFFER THIS ATTACK.
KEYWORDS: SOCIAL ENGINEERING. PHISHING. ATTACK. CYBERNETIC ENVIRONMENT. BRAZILIAN ARMY

REFERÊNCIAS BIBLIOGRÁFICAS

ARIMURA, Mayumi. Saiba a diferença entre Hackers, Crackers, White Hat, Black Hat, Gray Hat, entre outros. Disponível em: <https://egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros>. Acesso em: 22 maio 2020.

BRASIL AGORA. Golpe Whatsapp clonado pedindo dinheiro. Disponível em: <https://brasilagora.net.br/?p=1618>. Acesso em: 21 maio 2020.

CERT.BR. Golpes na Internet. Disponível em: <https://cartilha.cert.br/golpes/>. Acesso em 20 maio 2020.

COSSETTI, Melissa Cruz. WannaCry: tudo que você precisa saber sobre o ransomware. Disponível em: <https://www.techtudo.com.br/listas/2017/05/o-que-voce-precisa-saber-sobre-o-ran somware-wannacrypt.ghtml>. Acesso em: 21 maio 2020.

FREEPIC. Cadeado fechado no fundo digital, segurança cibernética Vetor Premium. Disponível em: <https://br.freepik.com/vetores-premium/cadeado-fechado-no-fundo-digital-seguran ca-cibernetica_5159323.htm>. Acesso em 22 maio 2020.

HALSEY, Mike. How Secure is Your Password? Disponível em: <https://www.ghacks.net/2012/04/07/how-secure-is-your-password/>. Acesso em: 22 maio 2020.

INTUIT ONLINE SECURITY CENTER. Phishing, Pharming, Vishing, and Smishing. Disponível em: <https://security.intuit.com/index.php/protect-your-information/phishing-pharming-vishing-and-smishing>. Acesso em: 20 maio 2020.

KASPERSKY. Dicas para a prevenção de phishing . Disponível em: < https://www.kaspersky.com.br/resource-center/preemptive-safety/phishing-prevention-tips>. Acesso em: 23 maio 2020.

KASPERSKY. Secure Password Check. Disponível em: <https://password.kaspersky.com/br/?utm_

medium=rdr&utm_source=redirector&utm_campaign=old_url>. Acesso em 21 maio 2020.

LOPES Nathamy. SOUZA Liliane. Médica cai em golpe no WhatsApp e recebe 'conselho' de bandido: 'Tem que amadurecer'. Disponível em: <https://g1.globo.com/sp/santos-regiao/noticia/2019/06/07/medica-cai-em-golpe-no-whatsapp-e-recebe-conselho-de-bandido-amadureca.ghtml>. Acesso em 20 maio 2020.

MAULAIS, Claudio Nunes dos Santos. Engenharia Social: Técnicas e Estratégias de Defesa em Ambientes Virtuais Vulneráveis. 2016. Projeto de pesquisa (Mestrado em Sistemas de Informação e Gestão do Conhecimento) - Universidade FUMEC, Belo Horizonte. Disponível em: <http://www.fumec.br/revistas/sigc/article/viewFile/3733/2031>. Acesso em: 22 maio 2020.

NETSPEED PORTAL EDUCAÇÃO. Qual a diferença entre phishing e pharming? Disponível em: <https://netspeed.com.br/mais/blog/empreendedorismo/empresarial/qual-a-diferenca-entre-phi shing-e-pharming-2/>. Acesso em 20 maio 2020.

PENSADOR. Kevin David Mitnick. Disponível em: <https://www.pensador.com/frase/ MTQ0MDcyNQ/>. Acesso em: 22 maio 2020.

PROOF. Como identificar um ataque de phishing em 9 passos. Disponível em: <https://www.proof.com.br/blog/politica-de-seguranca-da-informacao/>. Acesso em: 23 maio 2020.

PROOF. Spear Phishing: uma das ameaças mais efetivas. Disponível em: <https://www.proof.com.br/blog/spear-phishing/>. Acesso em: 21 maio 2020.

SILVA, Clayton S. et al. Engenharia Social: O Elo Mais Frágil da Segurança nas Empresas. Revista Eletrônica do Alto Vale do Itajaí. N° 02. Dezembro 2012. Disponível em: <http://www.revistas.udesc.br/index.php/reavi/article/view/2840/2172>. Acesso em: 23 maio 2020.

TERRA. Hackers desviam 520 mil euros do Boca Juniors. Disponível em: <https://www.terra.com.br/esportes/futebol/mercado-da-bola/hackers-desviam-520-mil-euros-do-boca-juniors-durante-transferencia-do-psg,467c82360a4db4f7b5fd74ce31821a52jgloipmc.html>. Acesso em 22 maio 2020.

Daniel Moura Felix Cardoso é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Capitão da Arma de Infantaria do Exército Brasileiro, Pós-graduado em Guerra Cibernética pelo Centro de Instrução de Guerra Eletrônica. Atualmente, exerce a função de Instrutor na Escola de Comunicações e pode ser contactado pelo email: felix.daniel@eb.mil.br.

Daniel Bomfim Nunes é técnico em eletrônica pela Escola de Sargentos de Logística (EsSLog). Sargento de Manutenção de Comunicações, está cursando licenciatura em Física na Universidade de Brasília. Atualmente, exerce a função de Monitor na Escola de Comunicações e pode ser contatado pelo e-mail bomfim.daniel@eb.mil.br

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

VANTAGENS OPERACIONAIS DO OFDM: ANÁLISE MATEMÁTICA E GRÁFICA COM SOFTWARE COMPUTACIONAL

David Justo Santos

Pós-Graduado em Gestão de Sistemas Táticos de Comando e Controle

Resumo: Este artigo está inserido no contexto de ciência e tecnologia e visa apresentar as vantagens operacionais e de segurança do uso da técnica de modulação OFDM. O propósito da pesquisa é fomentar a utilização de tal tecnologia pelo Exército Brasileiro, diante da evolução das tecnologias de comunicação de dados. Para isso, foram utilizados, como metodologia, revisões literárias de livros, artigos científicos e publicações de revistas científicas sobre as implementações do OFDM e seus avanços na realidade de comunicação digital, tendo sido feita a conferência das vantagens dessa modulação, com base na análise computacional e gráfica, utilizando-se o software Matlab. Buscou-se, como resultado, conciliar as vantagens de utilização do espectro de frequência, intrínseco ao OFDM, junto à confiabilidade e robustez necessárias a uma comunicação militar para o aprimoramento das comunicações quando do uso desta ferramenta. Por fim, conclui-se sobre a vantagem do emprego operacional, no Exército Brasileiro, dos equipamentos de comunicações de dados que empregam a referida tecnologia.

Palavras-chave: Multiplexação OFDM. Análise Computacional. Eficiência Espectral.

INTRODUÇÃO

Com o desenvolvimento da ciência e tecnologia envolvida nas comunicações digitais, e o aumento na quantidade de informação a ser transmitida (FRENZEL, 2015) em operações diversas do Exército Brasileiro e das Forças Auxiliares, tais como imagens e vídeos, faz-se necessária a análise das melhores formas de aproveitar o espectro de frequências à disposição e encaminhar a maior quantidade possível de informação.

A técnica abordada neste artigo é a OFDM, sistema consolidado e econômico de utilização do canal de comunicação que trabalha em conjunto com as modulações QAM e PSK na transmissão de sinais em W-LAN padrão IEEE 802.11a. (ROCHOL, 2012) (HAYKIN, 2009)

O avanço tecnológico de comunicação de dados permitiu, no Sistema Rádio Digital Troncaizado (SRDT) do Exército Brasileiro, por exemplo, a comunicação com o uso de sistemas de multiplexação e acesso de canais TDMA e FDMA permitindo um melhor uso da banda UHF de 800MHz. Tal banda permite a comunicação simultânea de diversos dispositivos, empregando-se apenas uma repetidora.

A relevância da pesquisa está ligada às vantagens de segurança frente à sistemas TDM, bem como à solução de problemas operacionais, enfrentados quando do uso de sistemas de multiplexação FDM, tais como: desvanecimento de canal, aproveitamento da banda de comunicação e robustez de sincronia de comunicação.

Buscou-se verificar se a utilização de um equipamento que utilize OFDM garante uma operação satisfatória quando em implementação real, analisando seu comportamento quando submetido a variações de ruído e resistência a falhas.

Vale esclarecer que as tecnologias TDMA e FDMA, citadas, são implementações de engenharia dadas pelos conceitos de TDM e FDM respectivamente. (ROCHOL, 2012) (L. PINTO, 2004)

O objetivo geral é apontar os problemas operacionais no uso do sistema de multiplexação FDM, apresentando as soluções contidas no OFDM, testando o processo de multiplexação e estimando um canal de comunicação via software Matlab e, com base nessa análise computacional, fomentar ou não a especificação de equipamentos com tal pro-

priedade, para as aquisições feitas pelo Exército Brasileiro.

Os objetivos específicos são: demonstrar e simular graficamente o funcionamento das multiplexações FDM e OFDM, mostrando sua vantagem operacional e robustez de segurança em comparação com o TDM; e construir um script computacional no Matlab capaz de estimar taxas de erros de bits quando utilizando o sistema OFDM, comparando-o com o modelo ideal.

O limite da pesquisa está centrado na análise do OFDM e seu comportamento em radiocomunicação quanto à transmissão em modulações digitais, aproveitamento da largura de banda e resistência à falhas operacionais.

1 METODOLOGIA

O métodologia do trabalho propõe a otimização de sistemas de comunicação, fomentando o uso de equipamentos que utilizem a multiplexação OFDM, através de análise bibliográfica e computacional, para melhor aproveitamento do canal de comunicação e para melhor aplicação operacional.

A pesquisa foi desenvolvida nos meses de março e abril do ano de 2019, tendo a análise gráfica sido realizada na etapa final do processo, no mês de maio.

O objetivo do estudo está centrado na evolução das comunicações e na necessidade de transmitir grande quantidade de informação em tempo real para as mais diversas atividades de comunicação pelo EB.

É importante destacar a necessidade de aprimoramento das técnicas de transmissão com a finalidade de atender às exigências crescentes de guerra cibernética e comunicações nas operações militares, com otimização do espectro de frequência pertinente à atividade militar, tarefa para o qual o sistema de multiplexação OFDM se apresenta como opção.

1.1 REVISÃO DE LITERATURA

Para desenvolvimento do artigo foi necessária a revisão literária sobre artigos e livros descrevendo o funcionamento do OFDM e literaturas de comunicação de dados.

Para análise de resultados foi utilizado o software matemático MATLAB.

Para o desenvolvimento dos algoritmos de simulação foi necessária a revisão avançada de conceitos de Geração de Sinais, Transformada de Fourier, Convolução de Sinais Digitais, Transformada Inversa de Fourier, Processamento de Sinais e Comunicação de Dados.

1.2 MULTIPLEXAÇÃO

Segundo ROCHOL (2012), a multiplexação é o processo que ocorre em consonância com a etapa de modulação, permitindo transmitir, simultaneamente, sinais diferentes na banda de frequência, separando as informações em canais de comunicação diferentes, aumentando assim a capacidade de informação a ser transmitida, como exemplo ressalta-se a necessidade de em muitos casos haver a transmissão concomitante de voz, dados e vídeos em uma comunicação digital de informação. (ABDOLI e MA J, 2015).

As técnicas de multiplexação mais comuns, em tradução literal, são a FDM, multiplexação por divisão de frequências, TDM, multiplexação por divisão de tempo e CDM, multiplexação por divisão de códigos. (ABDOLI e MA J, 2015)

Os avanços da tecnologia de comunicação trouxeram consigo a necessidade de melhor utilização da banda de comunicação de dados e a multiplexação OFDM tem se mostrado muito eficiente para este, de acordo com CORRÊA (2009), estando presente no desenvolvimento de dispositivos e tecnologias de W-LAN, segundo ARTHUR (2007), à qual a radiocomunicação está inserida.

O objetivo, todavia, é apresentar e

descrever as técnicas em discussão e apresentar as vantagens operacionais e de segurança que a técnica OFDM (Multiplexação por Divisão de Frequências Ortogonais), apresenta em comparação com as outras técnicas. Todavia, a técnica OFDM é uma evolução da técnica FDM e não caberá uma discussão quanto ao seu funcionamento em comparação com as técnicas TDM e CDM uma vez que suas implementações, funcionamento e problemáticas são diferentes.

2 RESULTADOS E DISCUSSÃO

2.1 MULTIPLEXAÇÃO FDM

De acordo com ROCHOL (2012), a técnica de multiplexação FDM divide a banda da frequência, BW, utilizada para modular a informação, frequência portadora, em frações que compartilham essa largura de banda de modo a enviar as informações por subportadoras, N. (HAYKIN, 2009). A banda é dividida de acordo com cada canal de informação a ser transmitida que no caso do canal de voz há uma ocupação de aproximadamente 4kHz, por exemplo. (HAYKIN, 2009)

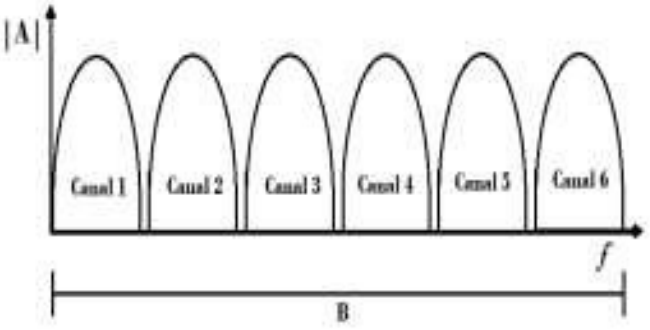
Dividindo a banda da frequência, BW, em vários canais de transmissão, Bs, sendo que estas novas bandas de frequência alimentarão diferentes circuitos de modulação com uma onda portadora para cada estágio. As frequências de subportadora são dimensionadas conforme o canal que se deseja trabalhar e costumam ser igualmente espaçadas entre si. (L. PINTO, 2004) (ABDOLI E MA J, 2015)

$$Bs = BW/N$$

O espectro resultante do sistema FDM é ilustrado nas figuras 1 e 2.

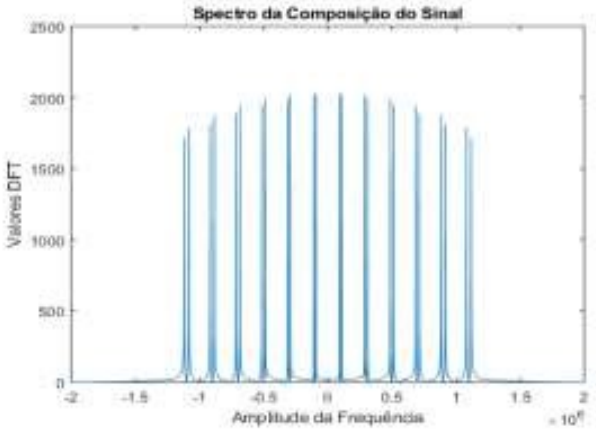
A multiplexação FDM além de otimizar a utilização da banda de frequência, possui vantagem sobre o sistema TDM quanto à segurança e robustez nas operações, pois não necessita de um sistema muito sofisticado de sincronização de canais quanto ao sistema TDM. (MINN, ZENG e BHARGAVA, 2015)

Figura 1 Espectro do Sinal FDMilus



Fonte: (HAYKIN, 2009)

Figura 2 Espectro do Sinal FDM Simulado



Fonte: Matlab/Autor

As desvantagens do uso do sistema FDM devem-se basicamente à restrição da duração dos símbolos enviados, uma vez que o aumento da duração do símbolo, Rs, diminuiria o tempo de símbolo, τ, pois a ocupação de banda se mantém nesse caso. (HAYKIN, 2009)

$$Rs = 1/\tau[baud]$$

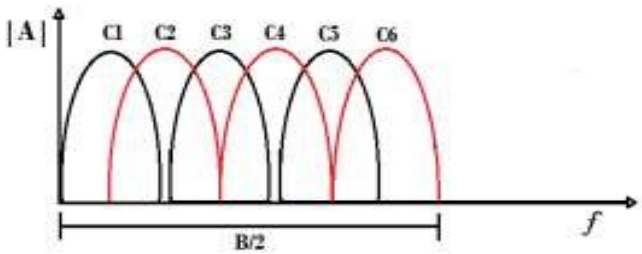
Outra desvantagem no uso do FDM deve-se ao aumento da probabilidade de interferência intersimbólica (ISI) e interferência intercanal (ICI), devido ao multipercurso dos diversos canais. (HAYKIN, 2009) (L. PINTO, 2004)

2.2 MULTIPLEXAÇÃO OFDM

A técnica de modulação *Orthogonal Frequency Division Multiplexing* (OFDM) é uma evolução da técnica de modulação FDM, tendo seu conceito proposto em 1968 e patenteado em 1970, segundo L. PINTO (2004), e implementação possível apenas a partir dos aos 2000 dada a evolução dos sistemas eletrônicos e de telecomunicações. (HAYKIN, 2009).

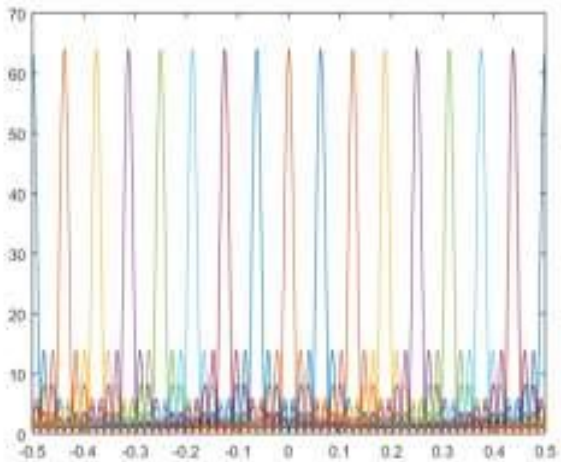
A multiplexação OFDM funciona separando os canais de transmissão em subportadoras, vide figura 3, como no FDM, de acordo com ROCHOL (2012) alterando, contudo, a banda utilizada para o mesmo fim pela metade de aproximadamente, segundo MINN, ZENG E BHARGAVA (2015) e IEEE (1999), uma vez que os canais estão ortogonais entre si, ou seja, não se faz necessário um ciclo de 180º para iniciar um novo canal, mas sim um ciclo de 90º, daí sua conceituação como ortogonal-FDM, comprovado pelo teste computacional da figura 4. (ROCHOL, 2012)

Figura 3 Espetro do Sinal OFDM ilustrativo



Fonte: (ABDOLI E MA J, 2015)

Figura 4 Espectro do Sinal OFDM Simulado



Fonte: Matlab/Autor

O sistema OFDM mantém as vantagens operacionais do FDM em relação à multiplexação TDM e o serviço de sincronização de modem. Todavia o sistema possui, igualmente ao FDM, problemas com ICI e ISI. (ABDOLI e MA J, 2015)

Para o problema de ISI, o OFDM possui a vantagem de reduzir a largura de banda em operação e com isso aumentar o tempo de símbolo. Todavia, uma solução para o problema de ICI, tanto para o circuito FDM quanto ao OFDM é a utilização de um intervalo de guarda, τ_g, que garante um espaçamento entre os canais na recepção e é dimensionado de acordo com a largura do canal. (ROCHOL, 2012) (HAYKIN, 2009).

Como relatado anteriormente o canal de comunicação, meio, impõe diversas perdas ao sistema tais como ruídos aditivos, ISI e ICI.

Contudo, uma dificuldade importante a ser enfrentada é o desvanecimento do canal, cujo o uso de subportadoras auxilia no enfrentamento, principalmente no que tange comunicações de rádio, cujo o canal de comunicação é o espaço livre que pode impor perdas significativas ao sistema comprometendo a recepção. ROCHOL (2012). O desvanecimento refere-se as atenuações sofridas no sinal transmitido pelo canal móvel, sendo ocasionado principalmente pelos vários obstáculos e variações naturais que o sinal percorre até chegar ao seu destino.

Assim sendo, o método proposto propõe demonstrar que, apesar de não haver controle sobre o canal, o uso de subportadoras garante uma comunicação eficiente se comparado a um sistema sem multiplexação.

Com o fim de comparar os métodos de multiplexação apresentados na metodologia foi utilizado o software matemático MATLAB, que realiza teste e análise matemática e gráfica de sinais, simulando uma transmissão de dados aleatórios e sua recuperação através de cálculos matriciais sucessivos e programados.

O OFDM possui aplicabilidade em sistemas diversos garantindo um uso mais eficiente da banda na comunicação de dados no que vale ressaltar sua evolução nos sistemas descritos no quadro 1.

Quadro 1 Aplicações do OFDM

Radiodifusão de Áudio Digital	DAB
Radiodifusão de Vídeo Digital	DVB
W-LAN Standart	IEEE 802.11A
Linha de Assinante Digital Assimétrica	ADSL

Fonte: (HAYKIN, 2009)

2.3 METODOLOGIA

Para analisar e comparar a eficiência do método OFDM, foi utilizado como método de análise de dados o software de programação Matlab e foram realizadas comparações de Taxa de erro de bit, BER, por Variação da Relação Sinal Ruído, SNR, para as variações da modulação QAM 16, 32, 64, 128 e 256, com e sem a etapa de multiplexação OFDM.

2.4 ANÁLISE

A eficiência do sistema foi verificada através de testes matemáticos comparando as curvas de BERxSNR com a modulação QAM, considerando maior transmissão de dados, robustez e segurança do sistema quando comparado ao uso da modulação PSK. (ROCHOL, 2012)

Variando a taxa de bits por símbolo, alterando o diagrama de constelação de 16 (4 bits), até 256 (8 bits) chaveamentos por ciclo, num total de transmissão de 10.000 (dez mil) bits gerados aleatoriamente, pode ser analisado e comparado o comportamento do sistema OFDM para um modelo ideal passando por um canal AWGN (Ruído).

A simulação sobre o modelo teórico ideal pode ser realizada no Matlab, mediante a ferramenta Bertool, sem a etapa de multiplexação OFDM.

A taxa de erro de bits (BER) é a relação de número de bits errados por número de bits transmitidos. (ROCHOL, 2012) (HAYKIN, 2009).

BER = (Nº de bits errados/Nº de bits transmitidos)

Já a relação Sinal Ruído (SNR) (ROCHOL, 2012) (HAYKIN, 2009), pode ser expressa pela seguinte fórmula:

SNR por bit ou Eb/No = Sinal/Ruído

Ou seja, quando aumentamos a relação sinal ruído temos mais presença de sinal em relação ao ruído e assim teremos uma tendência menor de erros de bit já que a SNR reduz para a casa de 10^{-6}, erro de 1 bit a cada 1.000.000 (1 milhão) de bits transmitidos.

Os testes realizados com o software Matlab demonstram que o sistema OFDM possui uma operação de comunicação aceitável para uma modulação 16QAM ou 32QAM, o que daria uma transmissão de 64 bits/ciclo ou 160 bits/ciclo, respectivamente, sendo o ciclo dado pelo período, T, da frequência de trabalho. (IEEE, 1999)

Pode ser observado, portanto, que considerando um sistema ideal, utilizando toda banda do canal, quando comparado ao sistema OFDM, demonstra que apesar da complexidade da multiplexação e considerando todo ruído percebido em um sistema de radiocomunicação convencional, ficou constatado que o sistema é aceitável dada as vantagens operacionais de largura de banda e transmissão de informação que ele oferece quando comparado ao sistema convencional, além da robustez contra o desvanecimento seletivo do canal.

CONCLUSÃO

Conforme apresentado e experimentado com o software MATLAB, a técnica OFDM, ao realizar uma multiplexação de origem serial em diversas subportadoras ortogonais moduladas individualmente com QAM, demonstrou eficiência e robustez ao ser percebida na recepção com taxas de erros aceitáveis para sistemas QAM 16 e 32, que são modulações complexas para radiocomunicação e com taxas muito além do necessário em comunicações com este fim.

Somada à simulada eficácia da multi-

plexação, existe a melhor ocupação da banda de transmissão, permitindo o uso de mais canais de comunicação e uma melhor resposta contra desvanecimento seletivo do canal.

Na prática, o OFDM oferece vantagens no uso do canal, tais como: a otimização sobre utilização da banda, maior capacidade de transmissão de dados e maior número de canais de comunicação.

Assim sendo, é aconselhável que em especificações de equipamentos rádio ou de enlace de dados em comunicações operacionais do Exército Brasileiro, as empresas fornecedoras sejam orientadas a oferecerem dispositivos com tal tecnologia, permitindo assim um uso mais amplo do espectro de comunicação. Todavia, faz-se necessário observar que este recurso é válido para comunicações de dados em banda UHF com sinal digital.

THE OPERATIONAL ADVANTAGES OF THE OFDM SYSTEM: MATHEMATICAL AND GRAPHIC ANALYSIS WITH COMPUTATIONAL SOFTWARE

Abstract. This article is inserted in the context of science and technology and aims to present the operational and safety advantages of the use of OFDM modulation. The purpose of the research is to foster the use of such technology by the Brazilian Army, given the evolution of communication technologies data. As a methodology, literature reviews of books, scientific articles and publications of scientific journals on the implementations of such technology and its advances in the reality of digital communication, having the conference of such facilities, based on a computational and graphic analysis of the multiplexing system in question, using Matlab computational software. As a result, it seeks to reconcile the advantages of using the frequency spectrum intrinsic to OFDM, together with the reliability and robustness required for military communication to improve communications when using this tool. Finally, to conclude whether the specification of data communication materials using such technology is advantageous in the operational use of the Brazilian Army.

Keywords: OFDM multiplexing. Computational Analysis. Spectral Responsible.

REFERÊNCIAS

[1] Frenzel Jr., **Louis E. Eletronic Communication Systems**. 4th ed. McGrawHill Education. 2015.

[2] (ROCHOL, 2012) Rochol, Juergen. **Comunicação de Dados**. Edição 01. Porto Alegre: Bookman, 2012.

[3] (HAYKIN, 2009) HAYKIN, S.**Communication Systems**. 5th ed. New York: John Wiley & Sons, Inc. 2009.

[4] Corrêa, Willian Câmara. **Estudos de sistemas OFDM para Comunicações Ópticas**. São Carlos: USP, 2012. 115f. Dissertação de Mestrado – Mestre em Ciências – Programa de Engenharia Elétrica, Universidade de São Paulo, São Carlos, 2012.

[5] Arthur, Rangel. **Novas Propostas para otimização de receptores de TV Digital baseados em OFDM em ambientes de Redes de frequência única regionais**. Campinas: Unicamp, 2007. 184f. Tese de Doutorado, Programa de Doutorado em Engenharia Elétrica, Universidade Estadual de Campinas, 2007.

[6] David, Rodrigo Pereira. **Técnica de Estimação de Canal Utilizando Símbolos Pilotos em Sistemas OFDM**. Rio de Janeiro: PUC, 2007. 132f. Dissertação de Mestrado – Pós-Graduação em Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro, 2007.

[7] L. Pinto, Ernesto; P. de Albuquerque, Cláudio. **A Técnica de Transmissão OFDM.** 2004. Disponível em: <http://www.cricte2004.eletrica.ufpr.br/ufpr2/tccs/27.pdf>. Acesso em: 15 mar. 2019.

[8] Abdoli J., Jia M. e Ma J., **Filtered OFDM: A New Waveform for Future Wireless Systems**, 2015 IEEE 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Stockholm, 2015, pg. 66-70.

[9] Minn, H.; Zeng, M.; Bhargava, V.K., **On timing offset estimation for OFDM systems**, Communications Letters, IEEE, vol.4, no.7, pp.242,244, julho de 2000

[10] Schmidl, T.M.; Cox, D.C., **Robust frequency and timing synchronization for OFDM**, Communications, IEEE Transaciones on, vol.45, no.12, pp.1613,1621, dezembro de 1997.

[11] IEEE Std 802.11a, Parte 11: **Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**, 1999.

O autor é bacharel em Ciências Militares pela Academia de Bombeiros Militar de Minas Gerais (ABMMG), Bacharel em Engenharia Elétrica pela Universidade Federal do Espírito Santo, (UFES). É pós-graduado em Eletrônica e Eletromecânica pela Universidade Cândido Mendes. Atualmente, exerce a função de Chefe da Seção de Manutenção Eletroeletrônica no Corpo de Bombeiros Militar do Espírito Santo (CBMES) e pode ser contatado pelo e-mail david.santos@bombeiros.es.gov.br

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

BENEFÍCIOS DO EMPREGO DO SOFTWARE RADIO MOBILE NO PLANEJAMENTO DO APOIO DE COMUNICAÇÕES

1º Ten Com Marcello Mamede Corrêa de Paula

Pós-Graduado em Gestão de Sistemas Táticos de Comando e Controle

RESUMO: O presente estudo buscou apresentar os principais benefícios do emprego do software de predição de enlaces Radio Mobile como ferramenta de auxílio ao planejamento do apoio de comunicações. O propósito do trabalho é difundir as capacidades desse software, possibilitando que os militares possam confeccionar seus estudos de enlaces com maior grau de confiabilidade e com maior eficiência. A metodologia utilizada foi a de pesquisa bibliográfica com a finalidade de aperfeiçoar ideias existentes sobre o assunto. Para isso, buscou-se a leitura de trabalhos científicos relacionados ao tema. O artigo apresentou as capacidades e limitações do Radio Mobile relacionadas às etapas da confecção do planejamento do apoio de Comunicações às operações desenvolvidas pelo Exército Brasileiro. Os resultados apontam que o Radio Mobile é uma ferramenta demasiadamente útil para os militares que têm a incumbência de elaborar um planejamento de enlaces por radiofrequência. Portanto, conclui-se que o Radio Mobile pode ser levado em consideração pelo oficial responsável pelo planejamento do apoio de comunicações, uma vez que colabora com a redução de falhas no planejamento do emprego do sistema rádio, além de servir como meio alternativo para ratificação dos enlaces.

Palavras-chave: Radio Mobile. Planejamento de Comunicações. Predição de enlace.

INTRODUÇÃO

O avanço tecnológico na área da ciência e tecnologia contribui para o desenvolvimento de muitas ferramentas computacionais que auxiliam nas telecomunicações. Com esse propósito, foi criado em 1997 o software Radio Mobile, um aplicativo com capacidade de prever a confiabilidade dos enlaces por radiofrequência.

No âmbito do Exército Brasileiro as transmissões por radiofrequência são de grande importância para as operações, pois proporcionam o envio oportuno das informações para todos os escalões, contribuindo para a execução do Comando e Controle.

Em grande parte das operações é necessário que ocorra, previamente, um planejamento detalhado do sistema rádio a ser utilizado. Nessa fase, o emprego do aplicativo Radio Mobile pode fornecer um apoio significativo e eficiente ao planejador.

Com essa premissa, a pesquisa possui o objetivo geral de apresentar os principais benefícios do emprego do Radio Mobile nos planejamentos dos apoios de comunicações.

Serão objetivos específicos: apresentar o aplicativo Radio Mobile, assim como suas capacidades e limitações; apresentar etapas da confecção de um planejamento de apoio de comunicações e mostrar a integração desse aplicativo com o referido planejamento.

Essa pesquisa não esgotará o assunto proposto, porém ela se torna bastante importante porque apresenta a possibilidade do uso dessa ferramenta por diversos militares que ora estarão confeccionando um estudo de transmissões via rádio, tornando mais confiável e eficiente.

Dessa forma, o propósito do trabalho é difundir para o Exército Brasileiro, mais especificamente aos militares da Arma de Comunicações, os aspectos positivos da utilização do aplicativo Radio Mobile como ferramenta auxiliar para confecção dos Planejamentos de Apoio de Comunicações.

1 METODOLOGIA

Este trabalho possui como problema norteador o seguinte questionamento: quais são os principais benefícios do emprego do Radio Mobile como ferramenta de auxílio no planejamento de Comunicações em Operações Militares?

Levando em consideração o problema apresentado, com o intuito de atingir o objetivo proposto, desde março de 2019, quando as pesquisas tiveram início, foi seguida uma abordagem qualitativa, estudando particularidades do tema proposto, buscando tendências e pensamentos acerca do tema, com observações.

A pesquisa foi de natureza aplicada, tendo em vista que não teve o objetivo de criar um conhecimento novo, mas sim, o estudo de pesquisas já existentes, que pudessem contribuir para o enriquecimento do trabalho e dar embasamento teórico e prático para as hipóteses do artigo.

A pesquisa foi conduzida de forma bibliográfica com a finalidade de aperfeiçoar idéias que já existem sobre o assunto. Buscou-se se a leitura e análise de fontes teóricas selecionadas, sejam elas em revistas, livros e trabalhos científicos, por meio físico e eletrônico.

Utilizando-se da pesquisa bibliográfica, em meados de março de 2019, deram início às pesquisas relacionadas ao funcionamento do Radio Mobile como ferramenta de predição de enlace rádio. Em seguida, no início de abril de 2019, foi feita uma consulta a alguns militares do Exército Brasileiro, especializados em comunicações, para levantar os principais equipamentos de radiofrequência utilizados pela Arma de Comunicações no Exército Brasileiro, compatíveis com o aplicativo Radio Mobile.

A próxima etapa foi estudar quais são as fases e como ocorre o planejamento do apoio de comunicações em uma operação militar do Exército Brasileiro, assim como levantar o principal responsável por essa tarefa no escalão nível brigada.

Por último, buscou-se uma ligação entre os planejamentos de apoio de comunicações e a ferramenta computacional de predição de enlaces rádio, de maneira que o uso desse aplicativo pudesse contribuir de maneira significativa para o emprego do sistema rádio em uma operação militar.

2 DISCUSSÕES

Nesta seção serão discutidos os resultados obtidos através da pesquisa realizada, de maneira a servir como embasamento teórico para as conclusões encontradas.

2.1 PREDIÇÕES DE RÁDIO ENLACE

Antes de ser abordada a definição de predição de rádio enlace, é necessário apresentar os significados de rádio enlace e de predição.

Felice (2005) afirma que o conceito de rádio enlace foi introduzido após as primeiras experiências de Guglielmo Marconi, um físico italiano, no final do Século XIX através da utilização das ondas curtas. Mas foi após a Segunda Guerra Mundial que foram desenvolvidos estudos no envio de sinais à longa distância utilizando as frequências em *Very High Frequency* (VHF), *Ultra High Frequency* (UHF) *e Super High Frequency* (SHF). No Brasil, esse conceito foi implantado somente em 1957, quando houve um enlace entre as cidades de São Paulo e Rio de Janeiro.

O rádio enlace pode ser definido como o estabelecimento de ligações de comunicações, feitas através de ondas eletromagnéticas entre duas estações rádio, existindo, obrigatoriamente, três elementos: um transmissor, um receptor e um meio de transmissão.

Após o entendimento do conceito de

rádio enlace, será apresentado o conceito de predição.

> Predição é o ato de predizer ou de afirmar o que se acredita que vai acontecer no futuro, ou seja, anunciar com antecedência o que pode acontecer. (MICHAELIS, 2019)

Sendo assim, predição de rádio enlace é um estudo feito por meio de um aplicativo para verificar se é possível o estabelecimento de uma comunicação por radiofrequência entre estações determinadas e o seu grau de confiabilidade.

> A predição de enlaces pode ser feita em qualquer faixa de radiofrequência, basta apenas, existir o aplicativo adequado para a faixa. No contexto das comunicações táticas do Exército Brasileiro, as bandas de VHF, UHF e SHF são utilizadas para transmissão de voz e dados em diferentes escalões de Comando e Controle e em diferentes plataformas: fixa, veicular e portátil (DIAS, 2018).

Devido à grande importância dessas faixas de frequência, este trabalho se restringirá às faixas utilizadas pelo Exército.

2.2 O APLICATIVO RADIO MOBILE

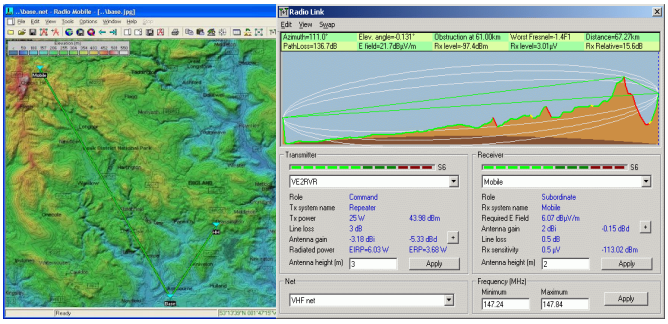
A utilização de recursos computacionais está cada vez mais difundida nos ramos da engenharia, trazendo maior confiabilidade e precisão aos projetos por meio de simulações cada vez mais realistas e vantajosas. Esses recursos são capazes de reduzir custos com protótipos e aumentar a prevenção contra erros no ambiente de operação.

Em telecomunicações é comum o uso de aplicativos que possibilitam a simulação de sistemas complexos de enlace de radiofrequência facilitando a organização e implementação.

Um desses aplicativos é o Radio Mobile, que é capaz de simular enlaces ponto-a-ponto ou simular áreas de cobertura. Sua primeira versão foi lançada em 1997 pelo Engenheiro Elétrico e radioamador canadense Roger Caudé, o qual definiu seu projeto como sendo uma ferramenta utilizada para prever o desempenho de um sistema de rádio. (COUDÉ,1997).

O Radio Mobile é uma ferramenta bastante utilizada por civis e militares, seja no meio acadêmico, seja no profissional. Além de gratuito, ele permite estudar a viabilidade de sistemas de radiofrequência para comunicação de voz e dados, na faixa de High Frequency (não ionosféricos), VHF, UHF e SHF. (OLIVEIRA et al., 2016). A figura 1 mostra uma das abas do aplicativo.

FIGURA 1 Tela do Radio Mobile
Fonte: Oliveira et al. 2016.



É uma aplicação altamente flexível e eficaz porque leva em consideração a topografia da região, condições climáticas, altitude, obstáculos e as especificações dos equipamentos, como a potência de transmissão, nível de sensibilidade, ganho de antena, distância de cabos, e a partir disso, consegue projetar grandes sistemas de telecomunicações.

O Rádio Mobile foi desenvolvido para cálculos de campo em sistemas móveis, utilizando o modelo de predição de Longley-Rice, que foi elaborado na década de 60 para predição em terreno irregular e vem sendo refinado ao longo dos anos.

Amaral (2012) diz que o modelo é baseado em dados coletados na faixa de frequência entre 40 MHz e 100 GHz, para antenas nas polarizações vertical e horizontal. O modelo de reflexão no solo com dois raios é usado para prever a potência de recepção dentro da linha de visada do rádio, que é a linha

com rádio visibilidade para um transmissor ou receptor, levando em consideração a curvatura terrestre e a refração atmosférica.

O modelo de Longley-Rice trabalha com dois modos diferentes a partir do perfil do terreno: quando os parâmetros inerentes do caminho são facilmente determinados, a previsão é denominada de previsão modo ponto a ponto, ou seja, ambos os terminais se encontram em locais específicos conhecidos. Nesse caso, o problema é basicamente estimar a potência de recepção. Caso o perfil do terreno não esteja disponível, o método de Longley-Rice apresenta técnicas para estimar os parâmetros específicos, e essa previsão é denominada previsão modo de área.

> O grande diferencial desse modelo de predição está no baixo custo computacional para a execução das rotinas de cálculo do somatório dos coeficientes de atenuação das faixas de linha de visada, difração e espalhamento (AMARAL, 2012).

O Radio Mobile trabalha na faixa de frequência de 20 MHz até 20 GHz e pode ser obtido, gratuitamente, em www.ve2dbe.com/rmonline.html.

Dentre as capacidades desse aplicativo, tem-se:

> a. permite montar cenários com diversas redes e sistemas de comunicação;
>
> b. combina bases de dados de elevação do terreno com cartas topográficas, imagens georeferenciadas e mapas externos como Google, VirtualEarth e Maplink;
>
> c. considera a influência do terreno, clima e ambiente (urbano ou rural) assim como as características dos equipamentos, cabos e antenas empregados;
>
> d. permite visualizar enlaces ponto a ponto assim como área de cobertura de transmissores, considerando postos fixos e móveis;
>
> e. possui capacidade de conexão a um GPS para obter informações de localização em tempo real;
>
> f. pode ser customizado pelo usuário de acordo com as necessidades da missão;
>
> g. possui interface amigável e em idioma Português. (CIGE, 2012, p.137)

Dentre as limitações do aplicativo, pode-se citar:

> a. o software não leva em conta o ruído (local, atmosférico e artificial) presente nas frequências dos enlaces;
>
> b. obstruções artificiais como edifícios e, naturais como árvores, não são levadas em consideração nos cálculos quando usando a base topográfica atual (SRTM3), que é livre e opera com células de resolução de 90m x 90m. (CIGE, 2012, p.137).

Cabe ressaltar que, atualmente, o Exército Brasileiro possui diversos equipamentos de radiofrequência compatíveis com essa ferramenta para planejamento de enlaces, dentre os quais se destacam os rádios da família Falcon III da Harris, como o RF7800V-HH e o RF7800M e os equipamentos da empresa Motorola, como o rádio portátil APX 2000 e a repetidora GTR 8000, ilustrados na figura 2.

FIGURA 2 Exemplos de equipamentos rádio empregados pelo Exército Brasileiro

Fonte: o autor, 2019.

2.3 PLANEJAMENTO DAS COMUNICAÇÕES

BRASIL (1997) afirma que o planejamento adequado e objetivo é essencial ao sucesso de qualquer operação militar. O planejamento apropriado permite o estudo detalhado e sistemático de todos os fatores envolvidos em uma operação projetada.

> O planejamento das Comunicações segue o processo normal de planejamento de Estado-Maior, começando com a missão e a diretriz do comandante, que levam à confecção do Estudo de Situação e dos demais documentos de Comunicações.
>
> O Oficial de Comunicações e Eletrônica é um dos membros do Estado-Maior e é responsável por assessorar o seu comandante no planejamento dos meios de Comunicações por ocasião das operações.Em seu planejamento devem ser considerados alguns aspectos condicionantes como:
>
> a) terreno - o terreno deve ser estudado de forma a permitir que sejam levantados, principalmente, os óbices ao estabelecimento dos diferentes sistemas e as soluções necessárias para a implementá-los.
>
> b) meios - em todos os escalões deve-se manter constantemente atualizadas, informações sobre a necessidade e disponibilidades dos meios de comunicações, tanto em pessoal como em material e o grau de adestramento em que as nossas tropas se encontram. A partir dessas informações pode-se planejar de modo a empregar judiciosamente os meios disponíveis, mantendo meios em reserva, fornecendo aos elementos subordinados e solicitando ao escalão superior quando for preciso.
>
> c) espectro eletromagnético - a utilização do espectro de frequências disponíveis, bem como as condições de propagação, embora sempre presentes no planejamento, influenciam mais, na medida em que tivermos que desdobrar um número maior de elementos no Teatro de Operações. (BRASIL, 1997)

Segundo BRASIL (1997), esse planejamento tem, normalmente, como a primeira etapa o estudo de situação, que se divide em 1ª e 2ª fases.

A 1ª fase é realizada no momento em que são elaboradas as linhas de ação pelos elementos do Estado-Maior, para o cumprimento da missão. Nesse momento são levantadas ideias que permitem concluir sobre quais as linhas de ação que poderão ser apoiadas pelos meios de comunicações, apontando as capacidades e as limitações de cada uma.

Após o comandante decidir qual será a melhor linha de ação, o estudo de situação segue para a sua 2ª fase. Nesse instante, são definidos de maneira detalhada todos os sistemas de comunicações a serem empregados durante a operação.

Para isso, alguns aspectos devem ser levados em consideração, como: o eixo de comunicações; previsão de deslocamentos e os meios capacitados para o apoio.

O próximo passo é o planejamento aprofundado de cada meio e a execução do reconhecimento de comunicações, que visa obter dados relevantes para o funcionamento adequado dos meios.

O militar responsável pelo planejamento do sistema rádio pode se valer de ferramentas de predição de enlaces, como o aplicativo já supracitado, para embasar seu estudo. Lembrando que os equipamentos devem operar entre a faixa de 20 MHz a 20 GHz para serem compatíveis com essa aplicação.

Sempre que for possível é interessante que seja realizado um reconhecimento no local onde os equipamentos rádio serão empregados. Deve-se utilizar essa oportunidade, antes do início da operação, para a realização de testes e para confirmação dos enlaces. Esses procedimentos ajudam a reduzir a probabilidade de falhas ao longo da missão.

É recomendado que antes de um reconhecimento e de testes no local, seja feito um estudo minucioso de cada parâmetro do sis-

tema de enlaces através do Radio Mobile. Ele será fundamental para a atividade, pois será capaz de definir os melhores locais para as instalações dos equipamentos, e também poderá mostrar uma área de cobertura com enlaces confiáveis.

Com os locais escolhidos e as predições realizadas com êxito, o Oficial de Comunicações e Eletrônica, responsável pelo planejamento, seguirá para a próxima etapa, a qual designará uma equipe especializada no material para verificar se aquele estudo realizado pelo Radio Mobile está condizente com a realidade.

Os rádios são capazes de transmitir voz e dados e são, na maioria das vezes, de grande importância para o êxito de qualquer operação. Não cabe, portanto, erros de planejamento que ocasionem a falta de comunicação rádio entre os militares durante a manobra militar.

Caso esse estudo no aplicativo não fosse realizado pelo planejador, a equipe de reconhecimento, mesmo sendo especializada, teria uma enorme dificuldade para selecionar os melhores pontos de instalação dos equipamentos. A predição realizada antes gera mais confiabilidade e fornece informações bastante relevantes para um reconhecimento de comunicações, como por exemplo, as regiões exatas para serem reconhecidas e quais os materiais específicos a serem empregados.

Outra ocasião a ser abordada é quando as operações militares se desenvolvem em terreno hostil, ou seja, dominado pelo oponente. Nesse tipo de caso, as chances da realização de reconhecimentos ou de testes dos equipamentos serão mínimas ou nulas, uma vez que as equipes responsáveis por essas atividades não são especializadas, nem possuem efetivo, para realizar infiltração em terreno inimigo, ou ainda, poderão colocar o sigilo da missão em risco.

Dessa maneira, cresce de importância a análise dos enlaces dos equipamentos de radiofrequência pelo Radio Mobile antes de cada operação. Essa será uma das poucas formas confiáveis de ratificar o planejamento de enlaces feito pelo Oficial de Comunicações e Eletrônica.

3 RESULTADOS

Para o êxito de uma operação militar, na maioria das vezes, é imprescindível que os meios de comunicações estejam operando em sua plenitude, pois dessa maneira os comandantes poderão realizar o comando e controle de maneira eficiente.

Dentre os equipamentos existentes, o mais usual e confiável é o rádio. Ele garante a transmissão de voz e dados por curtas e longas distâncias. Porém, para aumentar a probabilidade de sucesso das transmissões, é preciso que se tenha feito um planejamento apoiado no aplicativo Radio Mobile.

O resultado do emprego dessa ferramenta no auxílio de um planejamento pode trazer grandes benefícios, tais como:

a) aumento da confiabilidade no planejamento do militar, desde que esse tenha configurado todos os parâmetros necessários da maneira correta;

b) obtenção de dados relevantes e precisos para um reconhecimento de Comunicações;

c) meio alternativo para validação dos enlaces de radiofrequência quando existe algum tipo de restrição, como falta de pessoal, material, recursos orçamentários ou terreno hostil.

CONCLUSÃO

Após a descrição sobre o emprego do Radio Mobile no planejamento de Comunicações, conclui-se que existem grandes benefícios proporcionados por essa ferramenta computacional quando utilizada pelo Oficial de Comunicações e Eletrônica durante a elaboração de um sistema de transmissões por radiofrequência.

Dentre os benefícios apresentados, o que mais ganha destaque é o de ser usado como meio alternativo para confirmação de enlaces quando existe uma operação em terreno hostil, o que impede o oficial responsável pelo planejamento do emprego do sistema rádio enviar uma equipe ao local para reconhecimentos ou testes dos equipamentos.

Quando tal limitação ocorre, a maneira mais eficiente de validar o planejamento é se aproveitando das capacidades oferecidas pelo Radio Mobile, como por exemplo, de visualizar a área de propagação, mostrar o perfil topográfico do terreno e de retificar eventuais falhas no planejamento inicial. É certo que o aplicativo será bastante útil e imprescindível, pois, ao decidir não utilizá-lo, o planejador se limita a meios mais convencionais como carta topográfica e aplicativos como o Google Earth, que são obviamente menos eficientes, tendo em vista possuírem menos recursos técnicos.

Em todos os casos, não é recomendável deixar de realizar quaisquer tipo de estudo prévio ou realizar os testes com os equipamentos apenas durante o transcorrer da operação propriamente dita. Tais condições aumentam consideravelmente a possibilidade de ocorrências de falhas no planejamento do emprego do sistema rádio, fazendo com que a transmissão das informações, e por consequência o exercício do Comando e Controle, sejam comprometidas entre os diferentes escalões. Se erros dessa magnitude acontecem, a missão terá maior probabilidade de não atingir o seu estado final desejado.

Para futuros estudos, sugere-se uma comparação entre os aplicativos Radio Mobile e Path Loss, mostrando qual deles possui uma maior confiabilidade e apresenta um melhor desempenho para ser empregado como ferramenta de auxílio em planejamentos das comunicações.

Por fim, conforme os benefícios apresentados, o presente trabalho contribuiu para a área de Ciência e Tecnologia, demonstrando como uma ferramenta computacional pode auxiliar o Oficial de Comunicações e Eletrônica do Exército Brasileiro na elaboração de um planejamento de enlaces rádio em operações militares.

THE BENEFITS OF RADIO MOBILE EMPLOYMENT IN COMMUNICATIONS PLANNING

Abstract: The present study aimed to present the main benefits of using the Radio Mobile link prediction application as a tool to aid Communications planning. The purpose of the work is to disseminate the capabilities of this facilitator so that more military personnel can make their link studies more reliably and more efficiently. The methodology used was the one of bibliographical research with the purpose of perfecting ideas that already exist on the subject. For this, we sought to read scientific papers related to the topic. The article presented Radio Mobile, with its capabilities and limitations, and also, exposed parts of the preparation of a Communications Planning of the Brazilian Army. The results show that Radio Mobile is a very useful tool for those military personnel whose mission is to design a plan that contains radio frequency links. Therefore, it is concluded that Radio Mobile should rather be taken into consideration by the Planning Officer, in order to help considerably reduce the chances of system failures, and also serve as an alternative means of ratifying links.
Keywords: Mobile Radio. Communications Planning. Link Prediction.

REFERÊNCIAS

FELICE, Fernando. **Análise do desempenho de enlaces ponto-a-ponto utilizando a faixa de frequência não licenciada de 2,3 GHz em tecnologia Spread Spectrum.** Curitiba: UFPR, 2005.

PREDIÇÃO. **Dicionário online Michaelis**, 15 maio 2019. Disponível em < http://michaelis.uol.com.br>. Acesso em: 15 maio 2019.

DIAS, M. H. C; NAPOLITANO, Fillipe Machado Pinto; SILVEIRA, Arnaud Corrêa da. **Ferramenta de predição de cobertura para planejamento de comunicações táticas V/UHF**. Rio de Janeiro, set. 2018. Disponível em: < www.sige.ita.br > Acesso em: 17 abr. 2019.

COUDÉ, R. **Software Radio Mobile**. Disponível em <http://www.cplus.org/rmw/download/ download.html>. Acesso em: 04 abr. 2019.

OLIVEIRA, Thiago Carvalho de Barros; PAIM, Rodrigo Pippi; OLIVEIRA, Abel Peters de Assunção; WINK, Diego; ALMEIDA, Hamilton Rodrigo Gomes do Amaral Santiago. **Elaboração de um procedimento operacional padrão para configuração do software Radiomobile**.1 ed. Brasília, 2016. Apostila.

SANTOS, Vinícius dos. **Redes Wireless: Radio Mobile como ferramenta de predição de nível de sinal - Teoria e Prática**. Juiz de fora, 03 out. 2016. Disponível em: http://www.teleco.com.br/tutoriais/tutorialwirelessrb/default.asp>. Acesso em: 08 maio 2019.

AMARAL, Cristiano Torres do. **Uma análise do modelo de propagação Longley-Rice sob a perspectiva de ambientes urbanos localizados em área de clima tropical**. Belo Horizonte: UFMG, 2012.

ESCOLA DE COMUNICAÇÕES. **Propagação das Ondas Eletromagnéticas**. Brasília, 2019. Apostila.

CENTRO DE INSTRUÇÃO DE GUERRA ELETRÔNICA (CIGE). **Manual Escolar 2ª Fase - Fundamentos para a Guerra Eletrônica**. Brasília, 2012. 255 p.

ANJOS, A. A.; SILVA JUNIOR, R. A.; GOGLIATTI, R. **Dimensionamento de um sistema micro-ondas para distribuição de TV digital usando o software Radio Mobile**. IFMG, Formiga, jun 2014.

BRASIL, Ministério do Exército. **Portaria Nº 019-EME, de 14 de março de 1997:** Manual de Campanha Emprego das Comunicações. 2ª Ed 1997.

CRUZ, Carla; RIBEIRO, Uirá. **Metodologia Cientifica**: teoria e prática. Rio de Janeiro: Gisella Narcisi, 2002.

KÖCHE, José Carlos. **Fundamentos da metodologia científica**: teoria da ciência e prática de pesquisa. 18. ed. Petrópolis: Vozes, 2000.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de Metodologia Científica**. 3. ed. rev. e ampl. Sao Paulo: Atlas, 1991.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Concluiu com aproveitamento o curso de formação de oficiais e o curso básico de montanhismo. Atualmente, exerce a função de Adjunto do Chefe da 3ª Seção na 4ª Companhia de Comunicações Leve e pode ser contactado pelo email mamede.marcello@eb.mil.br.

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

A UTILIZAÇÃO DO MTO NO APOIO ÀS AÇÕES DE GERENCIAMENTO DE DESASTRES SOB A ÓTICA DAS RECOMENDAÇÕES DA UIT

1º Ten Com Felipe Gressana Martignago

Pós-Graduado em Gestão de Sistemas Táticos de Comando e Controle

RESUMO: Resumo: O presente trabalho buscou verificar a aplicabilidade da plataforma Módulo de Telemática Operacional como meio de apoio de comunicações em um contexto de ações de gerenciamento de desastres, visando responder o questionamento se o mesmo possui as capacidades técnicas necessárias que o permitem atuar nesse tipo de atividade. O propósito do artigo é iniciar tais estudos no uso do equipamento nessa vertente, haja vista a inexistência de publicações nesse viés. As metodologias utilizadas foram as de pesquisa bibliográfica e documental, onde foram coletados dados técnicos dos referidos equipamentos que fazem parte da plataforma em seus respectivos manuais e em publicações relativas ao apoio de comando e controle em situações de desastre, destacando-se a recomendação L.392 da União Internacional de Telecomunicações, além de diferentes artigos e relatórios técnicos relativos a uma plataforma de comunicações semelhante, projetada especialmente para situações de desastre. Os resultados apontam que o Módulo de Telemática Operacional não possui por completo a capacidade técnica para atuar em situações de desastres como preconizam as publicações de referência. Portanto, conclui-se que o material em questão tem condições de apoiar em comunicações um cenário de desastre, porém com limitações que somente podem ser vencidas utilizando-se de outros meios de maneira auxiliar.

Palavras-chave: Módulo de Telemática Operacional. Gerenciamento de desastres. Ajuda humanitária.

INTRODUÇÃO

O SISFRON emprega 75% de conteúdo nacional (BRASIL, 2015), além de atuar no desenvolvimento da Ciência e Tecnologia no país. Um dos principais produtos do projeto é o Módulo de Telemática Operacional (MTO), desenvolvido como meio de apoio ao C2 nas operações. Os benefícios do MTO para as missões de defesa da pátria do Exército são grandes. Todavia, o Exército Brasileiro também possui em sua responsabilidade as missões subsidiárias.

A LC nº 97/1999 dispõe sobre normas gerais da organização, preparo e emprego das Forças Armadas, balizando a ação delas em atividades não previstas na Constituição Federal, chamadas de missões subsidiárias (BRASIL, 1999). A cooperação com a Defesa Civil, prevista na referida lei no caput do artigo 16, foi o principal referencial utilizado na confecção do presente estudo, junto às especificações do MTO.

Assim, o presente trabalho insere o MTO no contexto da Defesa Civil, mais especificamente de apoio a desastres, visando cooperar com a resiliência das comunicações em situações dessa natureza.

Um avanço recente nessa área é a Diretriz de Iniciação do Projeto CCOp Mv, aprovada em janeiro de 2019 (BRASIL, 2019). Um dos cenários do uso do referido CCOp Mv é o apoio à Defesa Civil, sendo que o projeto se encontra no âmbito do Prg EE PROTEGER.

Diante dessas informações, observou-se a falta de publicações referentes ao uso do MTO em apoio às situações de desastre, existindo o questionamento se de fato o equipamento poderia se adequar tecnicamente a tal hipótese de emprego.

Portanto, a pesquisa possui o objetivo geral de realizar uma análise da capacidade técnica do MTO frente aos desafios da ajuda humanitária, mais especificamente ao gerenciamento de desastres naturais.

Foram objetivos específicos: enumerar as capacidades técnicas do MTO e analisar o que dizem as padronizações internacionais da União Internacional de Telecomunicações (UIT), levando-se em conta, também, outras publicações centradas na questão de teleco-

municações no gerenciamento de desastres.

O alcance da pesquisa é a análise das especificações técnicas do MTO, à luz das supracitadas publicações, limitando-se a verificar a sua adequabilidade como meio de apoio às telecomunicações em atividades de gerenciamento de desastre, sem realizar abordagem doutrinária dessa atuação.

O propósito do trabalho é iniciar o estudo do uso do MTO em situações de ajuda humanitária em sua vertente de Defesa Civil, justificando-se pelo fato de o EB possuir a já citada missão subsidiária e sendo relevante pelo fato de a Força ser continuamente requisitada pelas autoridades civis para complementar a capacidade de outros órgãos do Sistema Nacional de Proteção e Defesa Civil (SINPDEC).

1 METODOLOGIA

As metodologias utilizadas para produção desse artigo são as da pesquisa bibliográfica e documental.

A primeira se dá buscando em fontes teóricas já analisadas e publicadas, sejam elas em revistas, livros, enciclopédias, artigos científicos etc., incluindo-se também as fontes encontradas em meio eletrônico (FONSECA, 2002).

A segunda utiliza fontes mais diversificadas e por vezes sem tratamento analítico, como relatórios, manuais, documentos oficiais, dentre outros (FONSECA, 2002).

1.1 SEQUÊNCIA DAS AÇÕES

Utilizando-se de ambos os métodos, foram feitas pesquisas primeiramente relativas ao MTO e seus componentes, em meados do mês de março de 2019, utilizando-se como principal referência o material de treinamento do sistema disponibilizado pela empresa Harris (HARRIS, 2015). A análise dos dados dessa publicação foi realizada no ato de coletar e interpretar os dados técnicos de cada um dos componentes do Módulo, de maneira quantitativa.

Em paralelo, também no mês de março, buscou-se dados relativos à *Movable and Deployable Resource Unit* (MDRU), primeiramente no arcabouço da UIT. Durante a análise da documentação, procurou-se relacionar os conceitos que definem o equipamento em questão e o contexto onde ele seria utilizado, de forma qualitativa.

Durante o mês de abril foram estudados artigos e relatórios técnicos referentes a esse último assunto, alguns dos quais constam como referência da própria recomendação da UIT relativa à MDRU. Na análise dessa documentação, tanto qualitativa quanto quantitativa, foram relacionados os aspectos técnicos e modo de atuação específica dos equipamentos, de forma a serem encontrados os parâmetros necessários para a confecção do trabalho.

2 DISCUSSÕES

Nesta seção serão apresentados os resultados obtidos através da pesquisa realizada, de maneira a servir como embasamento teórico para as conclusões encontradas.

2.1 O MTO

O SISFRON foi concebido com o fim de se obter um sistema de sensoriamento e comunicações envolvendo radares, equipamentos rádio, sistemas de comando e controle e viaturas voltados para a vigilância das fronteiras do Brasil (HARRIS, 2015). Uma dessas viaturas é objeto de estudo desse trabalho, o MTO.

2.1.1 CONCEITO, CAPACIDADES E LIMITAÇÕES

O MTO consiste em um conjunto de equipamentos integrados em uma plataforma com grande mobilidade e flexibilidade num nível de comunicações táticas (HARRIS, 2015).

As capacidades do MTO se definem pela capacidade de seus componentes, que são em linhas gerais cinco: um rádio que opera em “linha de visada de alta capacidade”

(HCLOS, na sigla em inglês) para transmissão de dados numa velocidade de até 216 Mbps; um rádio que opera nas faixas de frequência VHF e UHF com transmissão de dados numa velocidade de até 10 Mbps e voz; outro rádio que atua como transceptor tático em VHF, também transmitindo voz e dados, porém em menor capacidade com 192 Kbps; um roteador com capacidade também de gerenciar chamadas de VoIP e por fim um dispositivo de ponto de acesso que opera de 2,412 GHz até 5,825 GHz, com capacidade de disponibilizar endereços de IP para dispositivos sem fio (HARRIS, 2015).

O roteador citado é do modelo Cisco 2921. Sua capacidade de gerenciar chamadas VoIP é semelhante àquela de um servidor dedicado, sem a necessidade de um hardware específico para executar tal função (HARRIS, 2015). Contudo, possui uma limitação de 450 telefones (CISCO, 2016) e 100 chamadas simultâneas (CISCO, 2017).

Com tais equipamentos, é possível o estabelecimento de enlaces a longas distâncias e com grande capacidade de transmissão de dados (especialmente com linha de visada) e voz, transformando o MTO em um poderoso nó de acesso para diversos meios e serviços em regiões onde não há tal infraestrutura ou não se deseja usar a estrutura local de telecomunicações por algum motivo. Tal potencialidade é de grande valia para a Força Terrestre, visto que, por diversas vezes, suas tropas atuam em regiões com tais características.

Somado a essas capacidades, vem a mobilidade proporcionada pela viatura operacional onde todo esse aparato se encontra. Por possuir perfil para atuar fora de estrada e também um gerador de energia solidário à cabine, a viatura base para o MTO permite grande raio de atuação e principalmente flexibilidade, sendo ambos princípios do comando e controle e das comunicações (BRASIL, 2018).

Como limitação, na parte técnica, o equipamento como um todo apresenta uma alta complexidade na sua operação, sendo necessária extensa capacitação de pessoal.

Outra limitação se dá em terreno muito acidentado ou montanhoso, onde não é possível o estabelecimento de ligações por visada direta, de maneira que o rádio que opera em linha de visada se torna ineficiente.

2.2 A UIT E SUAS RECOMENDAÇÕES

A UIT é atualmente a agência especializada em telecomunicações das Nações Unidas. Tendo se originado na junção da Conferência Telegráfica e da Conferência Internacional de Radiotelegrafia em 1932, assumiu o papel na ONU em 1947 (UIT, 2019).

A UIT se divide em três grandes setores de atuação: radiocomunicações, desenvolvimento e padronização (UIT, 2019). No presente trabalho foram analisados documentos provenientes do setor de padronização, as chamadas Recomendações.

As Recomendações da UIT têm por finalidade definir como operam e interoperam as diferentes redes de telecomunicações, e são divididas em diversas séries (UIT, 2019). Dentro de tais séries encontra-se a série “L”, que é novamente dividida, nela encontrando-se uma subdivisão dedicada para gerenciamento de desastres.

2.2.1 A RECOMENDAÇÃO L.392

Na referida subdivisão de gerenciamento de desastres, encontra-se a recomendação L.392 (UIT, 2016), que trata da utilização de unidades móveis de recursos de tecnologia de informação e comunicações (TIC) para melhorar a resiliência e a recuperação da rede em uma situação de gerenciamento de desastre.

Chamadas no documento de MDRU, essas estações móveis atuariam na substituição de infraestruturas de rede existentes, porém inoperantes, reproduzindo e possivelmente expandindo suas funcionalidades, tendo em vista o aumento da demanda em uma situação de desastre.

A MDRU visa atender não somente a população afetada pelo ocorrido, mas em especial as agências envolvidas nos trabalhos de ajuda humanitária no que tange ao estabelecimento do canal de comunicações e do comando e controle de tais ações (UIT, 2016).

A Recomendação L.392 não especifica em detalhes os requisitos mínimos a serem atingidos pela MDRU, mas trabalha em linhas gerais de que tipo de equipamento, características físicas e serviços disponíveis que essas unidades devem possuir para melhor cumprirem seus objetivos. Serão tratadas, no trabalho, os requisitos mais bem especificados pela Recomendação L.392.

O primeiro deles é a aparência externa. As MDRU devem ser resistentes ao stress de transporte, permanecerem operacionais mesmo quando embarcadas, possuírem capacidade de serem alimentadas pela rede de energia local, serem autossuficientes, terem tolerância sob diferentes temperaturas e umidade e terem capacidade de operar externamente ou em área coberta (UIT, 2016).

Outra característica é a conectividade externa. A MDRU deve possuir interfaces para conectar-se as estruturas rede através da rede principal (comercial) e também poder integrar-se as redes locais ainda operantes e seus terminais. Tal conectividade deve ser tratada tanto fisicamente (cabeamento de cobre, fibra ótica, rede sem fio, enlace satelital etc.) quanto logicamente (integrar-se através dos endereços de IP) (UIT, 2016).

Dentre os serviços que uma unidade móvel deve disponibilizar, destaca-se o serviço de telefonia. Em uma situação de desastre, este é um serviço solicitado tanto pela população civil quanto pelas organizações que trabalham nas operações de resgate. Uma das formas para sua implementação se dá através de um servidor VoIP presente na MDRU (UIT, 2016).

Outro serviço é o de Data Center. A Recomendação especifica que a MDRU deve oferecer acesso à internet através de canais temporários (como por exemplo o satélite). Contudo, caso esse canal não esteja disponível, a MDRU deve oferecer serviços de aplicações baseadas em Web e o gerenciamento de base de dados relativos a eles de igual maneira. Além de possibilitar a migração desses serviços e bases de dados para a Internet, quando esta se tornar disponível (UIT, 2016).

Por fim, a MDRU deve suportar um serviço de controle de tráfego de dados por prioridade. Sendo assim, chamadas de voz, por exemplo, gozariam de maior largura de banda. Nesse mesmo sentido, chamadas oficiais dos órgãos que atuam no desastre poderiam receber prioridade, enquanto serviços como streaming de vídeo para entretenimento seriam degradados (UIT, 2016).

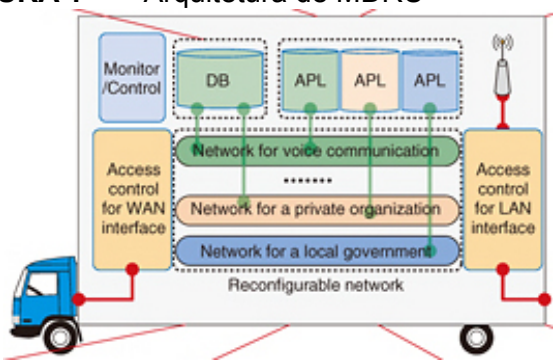
No presente trabalho, será tratado especificamente o serviço de VoIP, visto que em mais de uma das publicações de referência este é eleito o serviço mais importante que uma MDRU deve oferecer.

2.3 PUBLICAÇÕES RELACIONADAS AO TEMA

No que tange às especificações técnicas, a recomendação citada anteriormente (L.392) carece de dados mais precisos. Pelo fato de ser a primeira publicação reguladora relativa ao tema, sua abordagem é mais conceitual do que técnica. Todavia, outras publicações abordam mais detalhes quanto aos quesitos técnicos da MDRU.

Komukai, Kotabe e Sakano propõem em seu artigo de 2015 a arquitetura mostrada na figura 1.

FIGURA 1 Arquitetura de MDRU



Fonte: adaptado de Komukai, Kotabe e Sakano, 2015.

Como pode se observar na figura 1 e no referido trabalho, a unidade apresenta diversos componentes diferentes, que podem ser agrupados em quatro funções mais importantes: Conectar-se com a rede principal, oferecer conectividade através de rede sem fio, oferecer serviços baseados em IP – em especial o Voz sobre IP – e capacidade de link através de links diretos sem fio por microondas, chamados a partir desse momento no artigo de FWA – anteriormente referido como HCLOS.

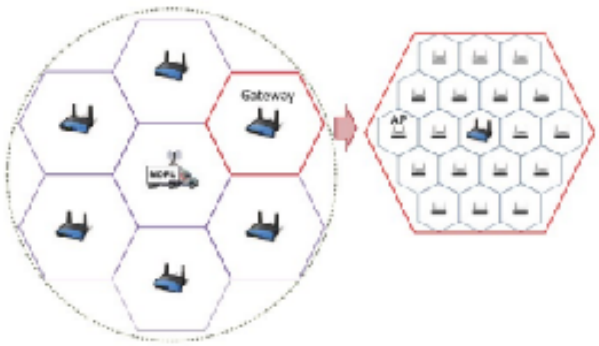
Quanto à conectividade com a rede principal, Komukai e Sakano (2015) sugerem duas opções: link satelital e conexão por fibra ótica. O primeiro pode ser obtido através de um equipamento de transmissão e recepção, cuja velocidade e largura de banda podem variar muito por motivos contratuais, ao ponto que os autores não mencionam detalhes em seu artigo.

A conexão por fibra ótica, por sua vez, permite maior velocidade e largura de banda, contudo não é tão facilmente obtida, em especial pela dificuldade de se conseguir informações sobre os parâmetros do cabeamento na área afetada pelo desastre. Para tal, Komukai e Sakano (2015) utilizaram um equipamento que pode imediatamente se conectar a qualquer tipo de fibra ótica que esteja funcional. O referido equipamento oferece uma capacidade de até 100 Gbps.

No que tange a oferecer conectividade a uma rede sem fio, a MDRU deve oferecer uma cobertura de 500 metros e acomodar até 5 mil usuários (NGO et al, 2013). Para atingir esses números, é utilizada uma abordagem hierarquizada na rede, de forma que esta cobertura seja dividida em 7 células hexagonais, seguida por uma subdivisão de cada célula em 19 outras células, conforme a figura 2.

Em cada uma das 19 subdivisões, a conectividade é realizada por um aparelho Access Point (AP) de 2,4 GHz, que por sua vez encaminha seu tráfego para o Gateway central da célula por um canal de 5 GHz, ao passo que o último é responsável por repassar todo o tráfego de sua célula para a MDRU. A conectividade MDRU-Gateway é realizada através de um link sem fio direto (FWA) de 25 GHz (KUMAGAI et al, 2015). Todo o material necessário para esses links é transportado junto da unidade móvel. Com esse tipo de arquitetura foi atingido um nível de confiabilidade de 95% em 25 diferentes cenários simulados (NGO et al, 2013).

FIGURA 2 Esquema de cobertura sem fio



Fonte: Adaptado de Ngo et al, 2013.

Dentre os serviços que podem ser disponibilizados, destaca-se o serviço de telefonia. Esse serviço é o mais requisitado em uma situação pós desastre, tanto pela população local quanto pelas agências governamentais por sua demanda por informação em tempo real (SEBAYASHI et al, 2014).

O sistema proposto em publicação de 2014 sugere a utilização do já citado sistema de conexão sem fio da MDRU para cadastramento e utilização do serviço de telefonia em VoIP. Os usuários utilizariam seus próprios dispositivos com tecnologia de conectividade sem fio (smartphones ou computadores) para acessar a rede e obter a aplicação, que em sua instalação já realiza o cadastramento e encaminha as informações para um banco de dados. Uma dessas informações é o próprio número de telefone comercial, de forma que a vítima do desastre o utilize para usufruir do serviço de VoIP, e pessoas em áreas não afetadas o usem para contatá-la como fariam normalmente (SEBAYASHI et al, 2014).

Enquanto a MDRU não possuir conectividade para fora da área afetada, as ligações podem ocorrer localmente e, após a tal conexão ser estabelecida, podem ser realizadas li-

gações em ambos os sentidos. Em pesquisa realizada com cerca de 300 pessoas que realizaram o teste do modelo proposto, 95% o consideraram útil ou muito útil (SEBAYASHI et al, 2014). As metas a serem alcançadas pelo sistema VoIP são as mesmas da conectividade sem fio: oferecer o serviço em um raio de 500 metros da MDRU e a um público de até 5 mil pessoas. Contudo, não foram citados requisitos mínimos de hardware para o referido servidor VoIP, apenas que o mesmo deve suportar uma carga de no mínimo 100 chamadas simultâneas (NTT AT, 2019).

Por último, a conectividade através de FWA é necessária por duas razões principais: a já descrita conectividade da rede sem fio em um raio de 500 metros da unidade, sendo necessário no mínimo seis pares de antenas para os enlaces que podem ser vistos na figura 2, e a possível conectividade entre várias MDRU, a fim de ampliar a rede para outras áreas afetadas (UIT, 2016). Esse último link não foi definido em termos de distâncias mínimas ou largura de banda, contudo foi utilizado em atividades de exercício com uma frequência de 25 GHz (KATO et al, 2019).

3 RESULTADOS

Com base nos dados apresentados, fica evidente que o MTO não possui todas as capacidades instaladas presentes na MDRU. São notáveis as semelhanças físicas dos dois equipamentos, como a rusticidade, flexibilidade e a relativa autossuficiência em relação à energia elétrica. Também quanto à capacidade de disponibilizar acesso a uma rede sem fio e de conectar outros módulos através de FWA, o equipamento do EB pode atingir parâmetros próximos aos propostos para a MDRU.

Contudo, o MTO possui consideráveis limitações das demais capacidades, em especial o oferecimento de serviços de Tecnologia da Informação (destacando-se a defasagem no serviço de VoIP, visto essa ser a principal funcionalidade da MDRU) e da conectividade externa por meio de fibra ótica, sendo capaz disso apenas por enlace satelital.

CONCLUSÕES

Após os estudos realizados sobre a definição internacional feita pela UIT sobre a MDRU, e diversas publicações que aprofundam os diferentes aspectos do referido material, conclui-se que o MTO não possui a capacidade plena de ser utilizado como um meio de apoio a uma situação de gerenciamento de desastre, sob a ótica das normas e trabalhos citados.

Porém, em situações específicas e dentro de suas limitações, o material pode possuir grande valor se utilizado como meio complementar, assumindo algumas funções que uma MDRU assumiria. A grande mobilidade, junto à alta capacidade de transmissão de dados em links de FWA, o estabelecimento de rede sem fio em seu entorno e um servidor VoIP de menor porte podem oferecer aos órgãos envolvidos com o gerenciamento do desastre importantes ferramentas de comando e controle.

Assim sendo, uma forma de se interpretar o resultado do presente trabalho está na capacidade do MTO de, em conjunto com outros meios de tecnologia da informação (como por exemplo servidores VoIP de maior porte e bancos de dados), servir de componente de uma estrutura conjunta e flexível de apoio e gerenciamento em uma situação de desastre. Cabe destacar que tal trabalho, em conjunto com outros órgãos em situações de calamidade, é missão subsidiária e encontra-se prevista em várias publicações, dentre elas O EXÉRCITO BRASILEIRO (BRASIL, 2014).

Como contribuição na área de gestão de telecomunicações em apoio às operações, o trabalho auxilia no balizamento para o planejamento de atuação dos militares e emprego dos meios de telecomunicação do Exército Brasileiro, em especial o MTO, no que tange ao apoio em Comando e Controle nas ações de gerenciamento de desastre. Possibilita ain-

da, em uma realidade específica de uma atividade de ajuda humanitária internacional, servir de referência para que a atuação em conjunto com órgãos de nações amigas ocorra da melhor forma possível, haja vistas as referências utilizadas, em especial a Recomendação L.392 da UIT e os demais artigos utilizados, vários dos quais a própria recomendação usa como referência.

Por fim, o artigo não esgota o assunto e poderá ser estendido e complementado em próximos estudos. Para esses, sugere-se um aprofundamento na interoperabilidade dos meios de comando e controle das diferentes agências que compõem o SINPDEC, visando a melhor gestão dos meios nesse tipo de atuação conjunto da Força Terrestre.

THE USE OF MTO AS A RESOURCE FOR DISASTER RELIEF FROM THE PERSPECTIVE OF ITU RECOMMENDATIONS

Abstract: The present work aims to verify the applicability of the Operational Telematics Module as a resource of communications support in the context of disaster relief actions, seeking to answer the question if it haves the technical capabilities needed which allows it to act in this kind of activity. The article's purpose is to begin such studies in the use of the equipment in this way, given the lack of publications in this bias. The methodologies used are the bibliographical and documental research, where the technical data collection was made about the equipment that are part of the platform, in the respective manuals, and the publications related of the command and control support in disaster situations, highlighting the Recommendation L.392 from the International Telecommunications Union, and also other articles and technical reports in a similar platform of communications especially designed for disaster situations. The results indicate that the Operational Telematics Module do not possess the full technical capacity to operate in disaster situations, as recommended by the reference publications. Therefore, the conclusion is that the material in question can do communications support a disaster scenario, but with limitations that can only be overcome by using other means in an auxiliary way.

Keywords: MTO. Disaster Management. Humanitarian Help.

REFERÊNCIAS

BRASIL. Exército. **As Comunicações na Força Terrestre** – EB70-MC-10.241. 1. ed. Brasília-DF: Comando de Operações Terrestres, 2018.

BRASIL. Exército. **Diretriz de Iniciação do Projeto Centro de Coordenação de Operações Móvel** – EB20-D-08.020. Brasília-DF: Estado-Maior do Exército, 2019.

BRASIL. Exército. **O Exército Brasileiro** – EB20-MF-10.101. 1. ed. Brasília-DF: EstadoMaior do Exército, 2014.

BRASIL. Lei Complementar nº 97, de 9 de junho de 1999. Disponível em: <http://www.planalto.gov.br/Ccivil_03/leis/LCP/Lc p97.htm>. Acesso em: 5 abr. 2019.

BRASIL. Ministério da Defesa. **SISFRON atua na defesa e no desenvolvimento da fronteira terrestre do Brasil**. 07 de dezembro de 2015. Disponível em: <https://www.defesa.gov.br/index.php/noticias/176 74-sisfron-atua-na-defesa-e-nodesenvolvimento-da-fronteira-terrestre-dobrasil>. Acesso em: 8 de maio de 2019.

CISCO. **Unified CME 11.5 Supported Firmware, Platforms, Memory, and Voice Products**. 29 de julho de 2016. Disponível em: <https://www.cisco.com/c/en/us/td/docs/voice_ip_ comm/cucme/requirements/guide/cme115spc.ht ml>. Acesso em: 20 de maio de 2019.

CISCO. **Cisco 2900 Series Integrated Services Routers**. 2017. Disponível em: <https://www.cisco.com/c/en/us/products/collater al/routers/2900-series-integrated-servicesrouters-isr/data_sheet_c78_553896.pdf>. Acesso em: 20 de maio de 2019.

FONSECA, J. J. S. **Metodologia da Pesquisa Científica.** Fortaleza: UEC, 2002. Apostila.

HARRIS CORPORATION. **Treinamento do Sistema MTO.** Versão 2.0, 28 de janeiro de 2015.

ITU. **Overview of ITU's History** (3). Disponível em:<https://www.itu.int/en/history/Pages/ITUsHistorypage-3.aspx>. Acesso em: 15 de abril de 2019.

_____. ITU-T **Recommendations**. Disponível em: <https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx>. Acesso em: 15 de abril de 2019.

_____. **What does ITU do?**. Disponível em: <https://www.itu.int/en/about/Pages/whatwedo.as px>. Acesso em 15 de abril de 2019.

ITU-T: L.392 - **Disaster management for improving network resilience and recovery with movable and deployable information and communication technology (ICT) resource units**. Genebra: ITU, 2016.

KATO, Nei; et al. **Development of Movable and Deployable ICT Resource Unit (MDRU) and its Overseas Activities.** Journal of Disaster Research. Vol. 14, n. 2, p. 363-374. 2019.

KOMUKAI, Tetsuro; KOTABE, Satoshi; SAKANO, Toshikazu. **Overview of Movable and Deployable ICT Resource Unit Architecture**. NTT Technical Review, Vol. 13, n. 5, mai. 2015.

KOMUKAI, Tetsuro; SAKANO, Toshikazu. **Highspeed and Plug-and-play Optical Interconnection for MDRUs**. NTT Technical Review, Vol. 13, n. 5, mai. 2015.

KUMAGAI, Tomoaki; et al. **Wireless access network system using M2M wireless access for MDRU**. NTT Technical Review, Vol. 13, n. 3, mar. 2014.

NGO, Thuan; et al. **Disaster Resilient Networking** – A new vision based on Movable And Deployable Resource Units (MDRUs). IEEE Network Magazine. Vol. 27, n. 4, p. 40-46, julago. 2013. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnu mber=6574664>. Acesso em: 2 de maio de 2019.

NTT AT. **Portable IP Telephone System for Disaster Situations.** Disponível em: <http://mdru.org/images/models/portableIPPBX_ pamphlet.pdf>. Acesso em: 6 de maio de 2019.

SEBAYASHI, Katsuhiro, et al. **Rapidly Deployable Phone Service to Counter Catastrophic Loss of Telecommunication Facilities.** NTT Technical Review, Vol. 12, n. 5, mai. 2015.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). É pós-graduado em Gestão de Sistemas Táticos de Comando e Controle e em Gestão em Ciência Política, Estratégia e Planejamento pela ADESG/IDESF/ESIC. Atualmente, exerce a função de Chefe da 3ª Seção na 15ª Cia Com Mec e pode ser contatado pelo e-mail martignago.felipe@eb.mil.br

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

APLICABILIDADE DA TECNOLOGIA 5G PARA USO DOS ÓRGÃOS DE SEGURANÇA PÚBLICA

José Ricardo da Assunção Ferreira

Mestrando em Telecomunicações e Redes de Comunicações

RESUMO: Os Órgãos de segurança pública vêm buscando cada vez mais um sistema de comunicações com flexibilidade, escalabilidade e sobretudo com altas taxas de dados e que suportem um número considerável de usuários. Nesse sentido a tecnologia 5G vem ao encontro desses anseios, pois além da taxa de dados e grande número de usuários, os sistemas necessitam que as novas tecnologia possam coexistir com as tecnologia já existentes. Garantindo assim a interoperabilidade entre os sistemas legados e a tecnologia 5G, isso devido a características de as redes 5G serem redes heterogenias. Por outro lado, a tecnologia 5G ainda possui muitos desafios a serem superados para sua efetiva utilização.

Palavras-Chave: 5G, Redes Heterogêneas.

INTRODUÇÃO

O Sistema Nacional de Comunicações Críticas (SISNACC) provê redes de voz e dados, com cobertura em todas as áreas geográficas de interesse do Estado Brasileiro, para atender os três níveis da administração pública nas ações de proteção pública, respostas a desastres, serviços de socorro e emergência e apoio à infraestrutura de governo nas atividades de fiscalização.

Esse sistema pode atender, ainda, de forma complementar, as estruturas de governo no setor da educação e saúde, as empresas de infraestrutura, bem como outras atividades estratégicas de utilidade pública de interesse do governo, sejam públicas ou privadas, tais como: ferrovias, hidrovias e mineração.

Nesse contexto, faz-se necessária a implementação do Sistema de Comunicações Críticas de modo a ser utilizado por todos os órgãos de segurança pública. Essa utilização racional visa diminuir os custos de implantação e de manutenção do sistema, por intermédio do uso compartilhado entre todos os interessados, com o consequente aporte de recursos por todos os usuários, racionalizando, assim, os custos de todos. Isso caracteriza o regime do uso em parceria.

Nesse sentido, a tecnologia 5G, devido a suas particularidades, é vista como uma solução altamente promissora no sentido de atender serviços de missão crítica, principalmente levando-se em consideração o grande fluxo de taxas de dados e um número muito grande de usuários.

Assim, essa rede deverá garantir a interoperabilidade, confiabilidade, segurança e disponibilidade às Forças Armadas, aos Órgãos de Segurança Pública, Fiscalização, Repressão e Controle e Defesa Civil, nos níveis federal, estadual e municipal, e também a outros usuários de interesse do Estado Brasileiro, melhorando a Segurança Nacional, com reflexos diretos na Defesa Nacional e possibilitando a ampliação do sistema, com redução dos custos, além de melhorar a gestão pública.

Inicialmente, no primeiro capítulo, será apresentada uma visão das principais características da tecnologia 5G aplicáveis na segurança pública. Na capítulo II serão apresentadas as principais tecnologias do 5G fundamentais para atender a demanda dos sistemas de comunicações dos Órgãos de Segurança Pública. No capítulo III será apresentado os principais desafios de implantação da tecnologia 5G e, por fim, será feita a conclusão deste trabalho.

1 TECNOLOGIA 5G

A seção que se segue tem como objetivo realizar uma revisão geral sobre a arquitetura e as tecnologia de acesso 5G, com o

enfoque em tecnologia aplicáveis a segurança pública.

1.1 COMPOSIÇÃO DAS VERSÕES E TECNOLOIAS

A arquitetura do sistema *Radio Access Network* (RAN) 5G será composta por versões evoluídas de 2G (GPRS / EDGE), 3G (HSPA / UMTS), 4G (LTE-Advanced / IEEE 802.16m), WLAN (WiFi), redes de espaço em branco na TV (TVWS), sem fio, óptico ou comunicações espaciais (FSOCs), telecomunicações tipo máquina (MTCs), fibra para casa (FTTH), rede óptica passiva (PON) e rede óptica.

Assim, cada camada terá tamanhos diferentes, definidos por diferentes estações base RAT (BSs), com capacidade de transmissão assimétrica, além de dinâmica de interferência complexa junto a um bloco de células ou dispositivos, respectivamente.

O Sistema 5G RAN consiste em vários grupos de redes heterogêneas (HetNets), cada camada terá tamanhos diferentes, definidos por diferentes estações base RAT (BSs).

A arquitetura do sistema 5G RAN é composta por macro células e pequenas células, retransmissores e comunicação dispositivo a dispositivo (D2D).

As macro células são compostas por estações base de alta potência (MeNBs) com potências de transmissão próximas a 43 dBm e ganhos de antenas próximos a 12-15 dBi [1].

Os MeNBs são adequados para aplicações em áreas amplas, como cobertura de comunicação para áreas remotas e rurais.

As micro células e pico células são compostas por estações base de baixa potência (μeNBs ou PeNBs) cujas potências de transmissão variam de 23 dBm a 30 dBm e ganhos de antenas de 0 a 5 dBi. Assim, devido às distâncias razoavelmente curtas, eles são adequados para aplicações urbanas e empresariais.

As femtocélulas são compostas por estações base implantáveis pelo consumidor (HeNBs) conectadas ao backhaul de banda larga dos consumidores, como PONs, FSOCs, etc.

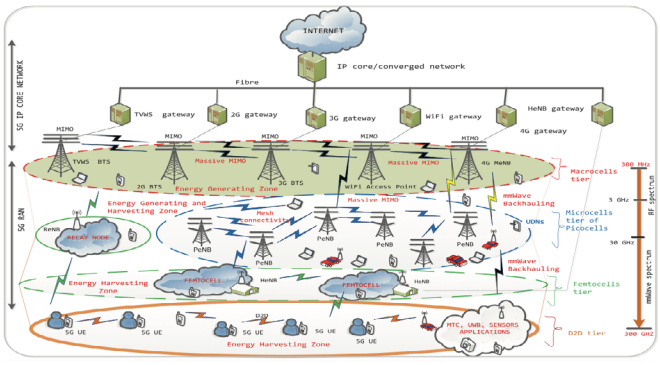
Os HeNBs podem transmitir com potências inferiores a 23 dBm e também podem ter associações de UEs restritas.

Finalmente, as comunicações D2D serão ativadas principalmente pelo espectro de microondas, essas comunicações podem diminuir o tráfego da BS.

2 BENEFÍCIOS DA TECNOLOGIA 5G

A utilização da tecnologia 5G vem para aumentar o número de usuários ao mesmo tempo em que aumenta significativamente, também o fluxo de dados. Esses benefícios incluem alocações de espectro muito maiores em bandas de espectro de frequência de ondas milimétricas não exploradas [2], [3], antenas maciças de direção de feixe altamente direcionais nos dispositivos móveis e nas BSs [4], [3], maior duração da bateria sustentada pelas técnicas de coleta de energia [1], comunicações full-duplex (FDCs) [5], menor probabilidade de interrupção, taxas de bits muito mais altas em porções maiores da área de cobertura, menor custos de infraestrutura e maior capacidade agregada [6], [7]. Na figura 1 vemos o LTE que compõem a rede 5G.

Figura 1 Arquitetura LTE da rede heterogênea 5G



Fonte: IEEE, 2016

Além disso, os meios guiados do sistema 5G RAN passarão principalmente de cobre e fibra para conexões híbridas de microondas sem fio, sem fio óptico e com fio (backhauling),

permitindo, assim, rápida implantação e conectividade em malha entre diferentes BSs.

Os sistemas 5G RAN irão adaptar-se a mais espectros de frequência (por exemplo, microondas ou banda de frequência extremamente alta (EHF), ou seja, 30 a 300 GHz, a fim de satisfazer aplicações de banda larga com denso tráfego de dados intra células. Isso implica em uma exploração maciça para utilização eficiente do espectro (EHF), complementarão o uso do espectro de ultra alta frequência (UHF) existente, ou seja, 300 MHz a 3 GHz . O principal motivo para essa alta exploração do espectro é a necessidade de atender às demandas de cobertura de comunicação de células mais amplas, mesmo além do 5G.

No gerenciamento da rede, as técnicas de redes definidas por software (SDN) serão aplicadas para dividir a rede geral (do núcleo para a RAN) em serviços de controle de sobreposição, principalmente no lado da rede principal. Os dados subjacentes da infraestrutura de encaminhamento de dados, principalmente no lado da RAN terá várias redes menores para atendimento da demanda de dados da rede heterogênea.

Por outro lado, com relação ao tratamento da taxa de dados, os planos de dados explorarão a utilização de antenas massivas de múltiplas entradas e múltiplas saídas (MIMO), a fim de concentrar a energia em regiões cada vez menores do espaço, com o objetivo de trazer grandes melhorias na taxa de transferência e na eficiência de energia irradiada.

Além disso, as técnicas massivas de MIMO criarão uma plataforma para o desenvolvimento de novos protocolos de acesso por rádio para o fluxo de tráfego heterogêneo, virtualizações de funções de rede (NFV), além de espectro conjunto e eficiência energética (SEE). O *backhauling* de fibra também deverá ser garantido para um sistema de comunicação de vários níveis.

Além disso, os sistemas 5G RAN satisfarão uma ampla variedade de requisitos e características de Qualidade do Serviço (QoS), como altas taxas de dados, mobilidade contínua, latência reduzida, alta confiabilidade, alta segurança e privacidade, alta duração da bateria do dispositivo e custos reduzidos do dispositivo.

Em termos da ampla variedade de requisitos, características e casos de uso de taxas de dados, os dados de vários Gbps devem incluir tablets em nós de acesso de alta e baixa potência. Dessa forma, centenas de taxas de dados de Mbps devem estar disponíveis para os consumidores finais em RANs 5G de várias camadas. Os casos mais gerais e os requisitos de QoS correspondentes exigirão que os componentes da rede sejam capazes de operar com larguras de banda de transmissão muito amplas (ou seja, 100 MHz) em bandas de frequência mais altas (ordem de 10 a 100 GHz) [3], para que as comunicações de curto alcance (ordem de dezenas a centenas de metros) possam ser utilizadas.

Os BSs de UDNs de rádio previstos, por padrão, serão densamente localizados, planejados de maneira precisa e transmitidos em baixas potências. As BSs dentro das pequenas células precisarão transportar tráfego sem fio das BSs de alta potência ou macro células para as redes de comunicação D2D ou redes de UEs. As BSs das UDNs devem ser capazes de gerenciar recursos de rádio de maneira eficiente e oportuna no lado de acesso dos sistemas 5G RAN tanto quanto forem necessários. Sendo assim, de uma forma geral, aplicam-se em situações em que o usuário interage e troca informações com a rede.

Os sistemas 5G RAN precisarão oferecer uma solução mais eficiente para permitir também que os dispositivos se comuniquem diretamente pelo link D2D, para dessa forma diminuir o trafego de dados para a BS, pois a comunicação D2D podem ser feita de forma direta.

3 TECNOLOIA 5G PARA A SEGURANÇA PÚBLICA

Os sistemas 5G possuem uma gama

de vantagens para a aplicação na segurança públicas. Desta forma, uma rede 5G pode oferecer vantagens como, por exemplo, melhor cobertura, devido ao investimento conjunto em apenas uma rede, além de remover problemas de interoperabilidade entre as agências com diferentes sistemas.

Além disso, a rede 5G também utiliza User Equipaments (UEs), como smartphones, e eNodeBs (estação rádio base), que também atendem a redes comerciais, diminuindo, dessa forma, os custos dos equipamentos, devido à escala global de produção (GSMA, 2018).

O 5G foi projetado para prover altas taxas de dados a partir de conectividade IP, com baixa latência, podendo ser utilizado por aplicativos com comunicação IP, permitindo que grandes números de serviços sejam fornecidos, como, por exemplo, consulta a banco de dados, streaming de vídeo e comunicação de voz (PTT e VoIP) em tempo real. Além disso, também foi projetado para fornecer uma taxa altíssima de dados para um número muito grande de usuários com máxima segurança e confiabilidade.

Sendo assim, essa tecnologia vêm ao encontro da necessidade das comunicações da segurança pública no sentido de um sistema versátil e muito seguro. Provendo uma taxa de dados bem maior do que as usadas com as tecnologia atuais.

Atualmente, o espectro alocado para aplicações de segurança pública no Brasil é de 5 MHz de upload e 5 MHz de download. O 5G pode ser utilizado com aplicações personalizadas para usuários de segurança pública, através de soluções baseadas em IP *Multimidia Subsystem* (IMS), como, *Push-to-Talk* (PTT) sobre telefonia celular. Podem ser implementados serviços de segurança melhorados e capazes de realizar transmissões ponto-multi-ponto de voz, vídeo e dados em comunicação PTT.

Além disso, a rede 5G, devido a sua arquitetura heterogênea em que é composta, também, por redes LTE, pode ser integrada as atuais redes *Land Mobile Radio* (LMR), viabilizando a convergência de tecnologia, e a convivência de serviços existentes, bem como serviços com necessidade de alta taxa de dados sobre uma mesma infraestrutura. Possibilitando, dessa forma, uma transição suave para uma futura implementação de uma rede heterogênea 5G.

Podemos utilizar também, a rede 5G de forma tática, com possibilidade de prover, temporariamente, cobertura em uma determinada região que necessite de comunicação crítica e de altas taxas de dados. Além disso, alguns recursos importantes para segurança pública podem ser integrados, como, por exemplo: drones, vídeos analíticos, viaturas autônomas, automação de dispositivos policiais, robôs conectados para atividades de risco (tais como a desativação de explosivos), inteligência de vídeos, aplicações de inteligência artificial e integração de imagens geradas por câmeras fixas e câmeras instaladas nos uniformes dos agentes (*bodycam*). Tudo isso só pode ser viabilizado com a alta taxa de dados e o grande número de usuários que a tecnologia 5G pode suportar.

4 DESAFIOS DA IMPLANTAÇÃO DO 5G

Levando-se em consideração a sua complexidade de instalação, um sistema 5G RAN heterogêneo deve ser capaz de lidar com operações de muitos sistemas de comunicação celular de várias camadas que são implantados dinamicamente e de maneira heterogênea combinando assim RAT diferentes e escaláveis.

Além disso, a sua arquitetura composta por várias tecnologias possui alta complexidade de gerenciamento dinâmico. Por esse motivo, essa implantação terá vários desafios técnicos rigorosos, com um cenário adverso de interferência eletromagnética de rádio e requisitos adicionais de gerenciamento de mobilidade dos usuários [8], [9].

Tem-se, ainda, os desafios das questões técnicas de sustentabilidade e escala-

bilidade da rede, pois os sistemas 5G RAN empregam os RATs de banda larga móvel existentes (2G, 3G, WLAN, 4G etc.) para operar. Os RATs também terão a capacidade de incorporar as BS *Full Duplex*, segundo as quais cada setor BS opera nos modos *Duplex* por Divisão de Tempo (TDD) e *Duplex* por Divisão de Frequência (FDD) [5].

Nesse sentido, tem-se a necessidade de utilização de antenas inteligentes com um número muito grande de elementos, bem como o uso de antenas direcionáveis (MIMOs massivos) [4], aprimorando, ainda mais, a eficiência espectral nas bandas UHF existentes, para níveis de serviço móvel em uma cobertura de área mais ampla, e bandas EHF, para níveis de serviço móvel em cenários específicos de casos de uso [10].

Outro desafio é a necessidade de coordenação entre BSs para atender às demandas dos grandes volumes de tráfego móvel.

Por outro lado, as implantações de redes ultra-densas (UDNs) serão necessárias para suportar os novos casos de uso como comunicações maciças do tipo máquina (MTCs), comunicações *multi-hop* (MHCs), comunicações ultrarrelegáveis (URCs), entre veículos e veículos para comunicações rodoviárias (V2RCs). Mantendo assim, a sustentabilidade, flexibilidade e escalabilidade da rede dos sistemas 5G RAN [2].

Para mitigação de interferência, as redes exigirão mecanismos mais sofisticados e seletivos de controle de interferência eletromagnética e gerência de recursos de rádio (bloco de canais) , para permitir que o sistema 5G RAN possa lidar com grandes volumes de tráfego e altas taxas de dados.

CONCLUSÃO

O emprego da tecnologia 5G para a aplicação na segurança pública, tais como: drones, vídeos analíticos, viaturas autônomas, automação de dispositivos policiais, robôs conectados para atividades de risco (tais como a desativação de explosivos), inteligência de vídeos, aplicações de inteligência artificial e integração de imagens geradas por câmeras fixas e câmeras instaladas nos uniformes dos agentes (*bodycam*) aliado à possibilidade de utilização da rede por um grande número de usuários com tráfego de dados de alta capacidade atenderá as necessidades dos órgãos de segurança pública. Nesse sentido, a tecnologia 5G proporcionará a tais órgãos melhores condições de realizar a sua missão constitucional que é a manutenção da paz social.

Tendo em vista a interoperabilidade entre os sistemas de comunicações existentes nos órgãos de segurança pública e as redes LTE, um aspecto muito relevante na utilização da tecnologia 5G voltada à segurança pública é a escalabilidade. Isso porque, como a rede 5G é uma rede heterogênea, ou seja, sua arquitetura é composta por diversas tecnologias incluindo o LTE, ela poderá coexistir com o legado de equipamentos já existentes e em operação pelos órgãos de segurança pública.

Por outro lado, para atender a demanda a qual a tecnologia 5G se predispõe a fornecer, existe uma série de desafios a serem superados para viabilizar a sua implantação. Atualmente existem vários estudos no sentido de buscar uma solução viável para todos os desafios de implantação da tecnologia 5G.

Dessa forma, a partir do momento em que a tecnologia 5G tiver seus desafios de implantação solucionados e sua utilização se tornar realidade, essa tecnologia ocasionará um impacto muito grande nos sistemas de comunicações dos Órgãos de Segurança Pública. Isso porque, tal tecnologia ampliará o sistema pré-existente, proporcionando maior escalabilidade, flexibilidade, segurança e confiabilidade, refletindo, assim, na melhoria dos serviços prestados pelos Órgãos de Segurança Pública e, consequentemente, trazendo melhorias para a sociedade brasileira.

APPLICABILITY OF 5G TECHNOLOGY FOR THE USE FOR PUBLIC SECURITY

ABSTRACT: PUBLIC SAFETY AGENCIES ARE INCREASINGLY LOOKING FOR A COMMUNICATIONS SYSTEM WITH FLEXIBILITY, SCALABILITY AND ABOVE ALL WITH HIGH DATA RATES AND SUPPORTING A CONSIDERABLE NUMBER OF USERS. IN THIS SENSE, 5G TECHNOLOGY MEETS THESE CONCERNS, BECAUSE IN ADDITION TO THE DATA RATE AND LARGE NUMBER OF USERS, THE SYSTEMS NEED NEW TECHNOLOGIES TO COEXIST WITH EXISTING TECHNOLOGIES. THIS ENSURES INTEROPERABILITY BETWEEN LEGACY SYSTEMS AND 5G TECHNOLOGY, DUE TO THE CHARACTERISTICS OF 5G NETWORKS BEING HETEROGENEOUS NETWORKS. ON THE OTHER HAND, 5G TECHNOLOGY STILL HAS MANY CHALLENGES TO OVERCOME FOR ITS EFFECTIVE USE.

KEYWORDS: 5G. HETEROGENEOUS NETWORKS.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] X. Lu, P. Wang, D. Niyato, D. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," IEEE Commun. Surv. Tuts., vol. 17, no. 2, pp. 757–789, Second Quart. 2015.

[2] T. S. Rappaport et al., "Millimeter wave mobile communications for 5G cellular: It will work!," IEEE Access, vol. 1, pp. 335–349, May 2013.

[3] S. Hur, T. Kim, D. J. Love, J. V. Krogmeier, T. A. Thomas, and A. Ghosh, "Millimeter wave beamforming for wireless backhaul and access in smallcell networks," IEEE Trans. Commun., vol. 61, no. 10, pp. 4391–4403, Oct. 2013.

[4] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," IEEE Commun. Mag., vol. 52, no. 2, pp. 186–195, Feb. 2014.

[5] S. Han, C. L. I, L. Dai, Q. Sun, and Z. Xu, "Full duplex networking: Mission impossible?," in Proc. Comput. Res. Repository, Oct. 20, 2014, pp. 1–6.

[6] C. X. Wang et al., "Cellular architecture and key technologies for 5G wirelesscommunicationnetworks,"IEEECommun. Mag.,vol.52,no.2, pp. 122–130, Feb. 2014.

[7] A. Agrawal, "Heterogeneous networks: A new paradigm for increasing cellular capacity," Qualcomm, Jan. 29, 2009. [Online]. Available: http://netseminar.stanford.edu/seminars/, accessed on Jan. 20, 2015.

[8] 3GPP TR 36.932, "Scenarios and requirements for small cells enhancements for E-UTRA and E-UTRAN," version 12.1.0, Mar. 2013.

[9] O.N.C.Yilmazetal.,"Smart mobility management for D2D communications in 5G networks," in Proc. IEEE Wireless. Commun. Netw. Conf. (WCNC'14), Istanbul, Turkey, Apr. 6–9, 2014, pp. 219–223.

[10] Ericsson, "5G radio access," Ericsson Rev., vol. 6, pp. 1–8, Jun. 18, 2014.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) e em Engenharia Eletrônica pelo Instituto Militar de Engenharia (IME). É mestrando em Telecomunicações e Redes de Comunicações pela Universidade de Brasília (UnB). Atualmente serve no Comando de Comunicações e Guerra Eletrônica do Exército e pode ser contactado pelo e-mail: ricardoferreiracmf@gmail.com.

ESCOM

Endereço

Estrada Parque do Contorno, Rodovia DF - 001, KM 5
Setor Habitacional Taquari - Lago Norte - Brasília - DF
CEP: 71559-902
Telefone: (0xx61) 3415-3532
(PABX) 3415-3502 (Voz/Fax)
www.escom.eb.mil.br