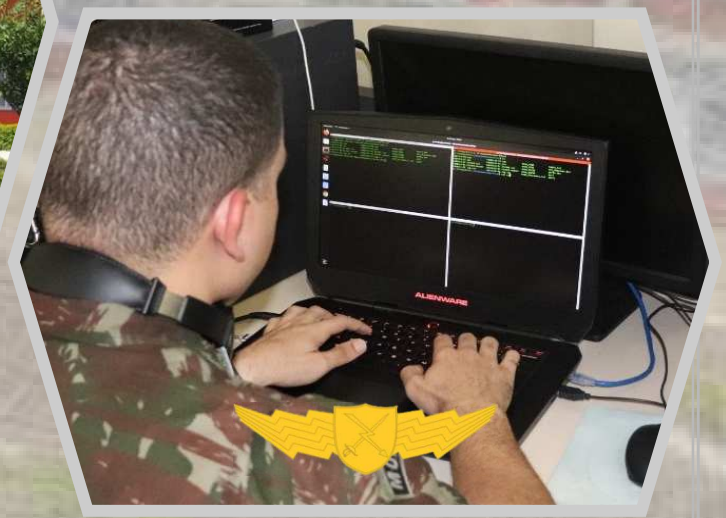
ISSN 0000-0000

DATA & HERTZ

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

ANO I, v. 1, n. 1 jan./dez. 2020

TURMA PIONEIRA do CIGE
1989



ISSN 0000-0000

DATA & HERTZ

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

ANO I, v. 1, n. 1 jan./dez. 2020

SUMÁRIO

Palavras do Comandante
Coronel Com Marcos Paulo Cardoso Nonato

Editorial
Tenente-Coronel Com Marco André de Almeida Maymone

Estudo sobre a Influência da Disposição Espacial dos Receptores de Guerra Eletrônica sobre a Precisão da Localização por TDOA
Capitão Com Leonardo Possideli Moreira

O Uso da Ferramenta SDNPWN como Forma de Pentest em uma Rede Definida por Software
1º Tenente QCO Lamartine Medeiros de Oliveira

Aplicação Operacional da RF em Fotônica: o enlace analógico a fibra óptica e a faixa dinâmica livre de espúrio
Capitão Com Bruno Elias Ribeiro

Funcionalidade dos Software e Hardware Livres na Localização de Sinais: estudo de caso, analisando o uso do SDR-RTL pelo método TDOA
Capitão -Tenente (Marinha do Brasil) Pedro Tebaldi Medeiros da Silva

O Processo de Elaboração da Lista de Alvos Cibernéticos no Nível Tático
Tenente-Coronel Com Vinícius Lacerda Vasquez

Atuação colaborativa da Defesa Cibernética na proteção de infraestruturas críticas de interesse para a Defesa Nacional
Tenente-Coronel Com Walbery Nogueira de Lima e Silva

Centro de Instrução de Guerra Eletrônica (CIGE)

Comandante
Cel Com Marcos Paulo Cardoso Nonato

Subcomandante
Ten Cel Marco André de Almeida Maymone

Divisão de Ensino
Maj Com Ezequiel da Silva Bastos

Seção de Guerra Eletrônica
Maj Com Fernando Henrique Castellani

Seção de Guerra Cibernética
Maj QCO Thiago André Baldissera

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

Seção de Meios Auxiliares de Instrução (SGMAI)
1º Ten Com Marcelo da Silva Polverari

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

DATA&HERTZ – Revista Científica de Guerra Eletrônica e Guerra Cibernética do Centro de Instrução de Guerra Eletrônica / Centro de Instrução de Guerra Eletrônica.
v. 1, n. 1, jan./dez. 2020 - Brasília-DF

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

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

CDD 350

Centro de Instrução de Guerra Eletrônica (CIGE)
Revista Científica do Centro de Instrução de Guerra Eletrônica – Data & Hertz

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

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

OBJETIVOS

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

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

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

PÚBLICO-ALVO

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

PUBLICAÇÃO DE ARTIGOS

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

PROCESSO DE AVALIAÇÃO

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

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

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

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

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

DATA & HERTZ
Revista Científica de
Guerra Eletrônica e Guerra Cibernética
do Centro de Instrução de Guerra Eletrônica

PALAVRAS DO COMANDANTE

O Centro de Instrução de Guerra Eletrônica (CIGE) mais uma vez se lança em uma empreitada em prol da difusão do conhecimento. Tal tradição, herdada dos Pioneiros deste Centro criado a mais de trinta e cinco anos, mantém vivo o lema de inovar e capacitar.

O CIGE, estabelecimento de ensino àvido por novos desafios, somou ao título de "Álma Máter da Guerra Eletrônica" o de "Berço da Guerra Cibernética" ao explorar, já em 2012, o espaço cibernético.

Hoje nosso Centro tem como missão capacitar os recursos humanos necessários às atividades de Guerra Eletrônica, Inteligência do Sinal e Guerra Cibernética, cooperando com a evolução doutrinária nessas áreas por meio de cursos, estágios, atividades de pesquisa e programa de pós-graduação. Portanto, esta publicação vem corroborar para que possamos cumprir as obrigações que norteiam nossos esforços.

Assim sendo, esta Revista tem por objetivo a divulgação dos trabalhos de instrutores e alunos, disseminando conhecimento, elucidando dúvidas e, quem sabe, atraindo novos interessados, incentivando talentos a se juntarem aos especialistas em Guerra Eletrônica e Defesa Cibernética.

Dessa forma, buscou-se apresentar trabalhos de fácil entendimento em uma linguagem atrativa e palatável, sem perder o conteúdo, core de qualquer produção científica.

Cabe destacar, ainda, os militares que tiveram seus artigos selecionados. Os trabalhos foram elaborados por profissionais com espírito inovador aguçado, elevado interesse pela pesquisa e visão de futuro inigualável, transformando seu esforço intelectual em um produto rico, capaz de prender a atenção de especialistas e leigos.

Por fim, desejo a todos uma boa e proveitosa leitura!

Coronel Com Marcos Paulo Cardoso Nonato

Diretor de Ensino

DATA & HERTZ

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

EDITORIAL

Caro leitor,

Este ano estamos lançando a revista científica do CIGE com o principal intuito de divulgar as pesquisas científicas realizadas aqui. "Data&Hertz" foi o nome escolhido para a revista, pois ela significa a sinergia nas áreas de Guerra Eletrônica e Guerra Cibernética.

Esta sinergia está associada ao rápido desenvolvimento tecnológico obtido pela humanidade. Nestes últimos anos houve uma evolução tecnológica nunca antes imaginável. Smartphones, tablets e computadores mudaram os hábitos da sociedade. Em um curto espaço de tempo, a tecnologia explodiu e agora muitas pessoas não conseguem imaginar uma vida sem ela. Olhando estas mudanças foi que o ensino no Exército evoluiu ligado a este desenvolvimento tecnológico. O Sistema de Educação e Cultura do Exército tornou-se, então, fundamental na capacitação e no desenvolvimento das competências desejadas para o profissional militar do futuro.

A Diretriz Estratégica de Ensino do Exército Brasileiro afirma que o Sistema de Ensino baseia-se no princípio da continuidade da aprendizagem ao longo de toda a carreira do militar. O ensino, além de preparar os recursos humanos para suprir as necessidades da Força, deve capacitar o militar a interagir, em todos os níveis, com a sociedade brasileira. O aluno é a figura principal do processo ensino-aprendizagem e deverá ser estimulado a buscar a auto-aprendizagem, estando permanentemente em condições de absorver novos conhecimentos.

As novas tecnologias estarão presentes em todas as atividades e se constituirá como um dos principais elementos de inovação das metodologias do ensino. As tecnologias da informação e comunicações permitirão um elo entre os estabelecimentos de ensino e os seus alunos, proporcionando maior atratividade e a necessária interação.

Com esta perspectiva de inovação, constituindo pontos-chave e eixos construtivos do processo ensino-aprendizagem, o CIGE parte para a introdução de novas práticas metodológicas no ensino, aplicando conceitos interdisciplinares das demais áreas do conhecimento humano, explorando as potencialidades de novas tecnologias e revisando conceitos sobre as práticas da avaliação do aprendizado.

Diante do exposto, esta revista pretende contribuir com a inovação tecnológica ao divulgar os artigos científicos produzidos por nossos alunos e colaboradores. Nesta revista estamos certos de que há ainda muito caminho a ser seguido, mas confiantes de que o primeiro passo já foi dado. Por isso, boa leitura!

Tenente-Coronel Com Marco André de Almeida Maymone

Subdiretor de Ensino

A influência da disposição espacial dos receptores de Guerra Eletrônica sobre a precisão da localização por TDOA

Cap Com Leonardo POSSIDELI Moreira*

RESUMO

O presente trabalho realiza o estudo preliminar sobre a influência da disposição espacial dos receptores sobre a precisão da localização eletrônica por Time Difference of Arrival (TDOA). A análise foi realizada considerando um ambiente bidimensional (xOy) sobre a influência de um canal com desvanecimento por multipercurso. O algoritmo de localização foi baseado no método de Chan e foram testadas as geometrias em linha, em cunha, em cunha invertida e circular, a fim de identificar variáveis que se relacionam com a raiz do erro quadrático médio (RMSE) da localização. Os resultados demonstram a influência do ângulo de interseção entre hipérboles sobre a precisão dos resultados. Para as geometrias em cunha e circular parece existir uma relação inversa entre o ângulo de interseção e o RMSE da localização, apresentando maior precisão para os ângulos próximos a 90º. Outras variáveis espaciais, tais como a distância e a forma do arranjo, também influenciam a precisão. O arranjo em linha não apresentou resultados válidos pelo método de Chan, sendo descartado desse estudo. As conclusões foram estruturadas de forma a identificar premissas para otimizar o posicionamento dos receptores com o intuito de aumentar a precisão dos resultados.

Palavras-chave: Localização eletrônica. TDOA. Geometria.

Influence of the spatial arrangement of the receivers of Electronic Warfare on the accuracy of the location by TDOA

ABSTRACT

This paper presented a preliminary study on the influence of geometries of receivers on the accuracy of the location by Time Difference of Arrival (TDOA). For analysis was considered a two-dimensional environment (xOy) in an channel fading by multipath. The location algorithm was based on the method of Chan and were tested the geometries in a line, curve, inverted curve and circular to identify space variables that are related to the root mean square error (RMSE) of the location. The results demonstrated the influence of the intersection angle between hyperboles. For circular and curve geometries was observed an inverse relationship between the angle of intersection and the RMSE, with greater precision for angles near 90°. Other spatial variables such as the distance and shape, also influence the results accuracy. The line geometry did not provide valid results by the method of Chan. The conclusions have been structured to identify rules to optimize the placement of receivers in order to increase the accuracy of the results.

Keywords: *Geolocation. TDOA. Geometry.*

1 INTRODUÇÃO

O Exército Brasileiro intensificou sua participação nos últimos anos em operações de não-guerra em ambiente urbano, por exemplo, Operação Arcanjo na região do Complexo do Alemão, Operação São Francisco no Complexo da Maré, ambas na cidade do Rio de Janeiro-RJ, e Operação de Segurança da Copa do Mundo de 2014, abrangendo cidades em todo o território nacional.

A atividade de Guerra Eletrônica esteve presente nessas operações como fonte de informação a partir do sensoriamento do espectro eletromagnético e da localização eletrônica de ameaças.

No entanto, a atuação em cenário urbano acentua o erro de localização devido ao aumento do ruído eletromagnético e a grande densidade de obstáculos, por exemplo, prédios, automóveis, aeronaves e pessoas, que determinam um canal com desvanecimento por multipercurso.

A velocidade com que uma ameaça é identificada e contida depende do tamanho da região da localização, que, por sua vez, está diretamente relacionada aos erros inerentes ao sistema, das características do canal de transmissão e da disposição espacial dos receptores.

A diferença de tempo de chegada (TDOA) apresenta-se como uma das técnicas empregadas pelos sistemas de localização para determinar a posição de um transmissor.

Considerando a incapacidade de alterar as características do canal ou do sistema de guerra eletrônica, seria possível reduzir o tamanho da área de localização posicionando adequadamente os receptores com o intuito de atingir a maior precisão.

No entanto, entende-se que a falta de informações a respeito da influência da disposição espacial sobre a precisão do resultado, poderá ocasionar o posicionamento inadequado do arranjo, reduzindo sua capacidade para detectar ameaças.

Dessa forma, esse estudo buscou identificar regras para otimizar a escolha da posição dos receptores e aumentar a precisão da localização eletrônica de ameaças.

2 LOCALIZAÇÃO POR DIFERENÇA DE TEMPO DE CHEGADA (TDOA)

Os estudos sobre a localização eletrônica por TDOA iniciaram durante a Segunda Guerra Mundial motivados pela necessidade de criação de um sistema de navegação. Nesse período foi desenvolvido o *Long Range Navigation* (LORAN) que possibilitou a determinação da posição do receptor em um plano de duas dimensões a partir de três transmissores conhecidos e sincronizados.

Atualmente esse sistema foi substituído pelo Sistema de Posicionamento Global (GPS) que possibilita a localização em três dimensões, contudo o modelo matemático que determina a posição continua essencialmente o mesmo (COMPAGNONI; NOTARI, 2014).

A localização por TDOA não necessita conhecer o tempo em que a emissão originou-se para estimar a posição do transmissor (MUÑOZ, 2009). Essa característica é uma vantagem sobre outros métodos de localização baseados no tempo de chegada (TOA), possibilitando o seu emprego na atividade de guerra eletrônica, uma vez que a informação sobre o tempo em que o sinal foi transmitido é desconhecida para o sistema de monitoração.

A localização da fonte ocorre a partir do cruzamento de duas ou mais curvas da hipérbole geradas a partir de múltiplas medidas extraídas por meio da mudança da posição dos receptores ou acrescentando mais elementos ao arranjo. A localização em três dimensões pode ser realizada por meio da interseção de hiperbolóides geradas em um plano Oxyz.

Matematicamente, a diferença do tempo de chegada da onda eletromagnética, determinada a partir de dois receptores posicionados em um plano euclidiano xOy nas posições $P_1(x_1,y_1)$ e $P_2(x_2,y_2)$, define uma hipérbole com focos em P_1 e P_2na qual uma de suas curvas contêm a posição do transmissor $T(x_t,y_t)$ *(COMPAGNONI; NOTARI, 2014)*.

A localização é definida pela interseção de duas ou mais hipérboles, definidas por um conjunto de no mínimo 3 (três) receptores.

As equações de cada hipérbole formam um sistema não-linear que exige métodos específicos para linearização a fim de determinar o ponto de interseção.

Devido a sua característica de não linearidade, um arranjo formado por apenas 03 (três) receptores em um plano 2-D e por 04 (quatro) para um plano 3-D poderá determinar mais de uma região de interseção, demonstrando ambiguidade nos resultados. A literatura identifica essa situação como *bifurcation problem.(COMPAGNONI; NOTARI, 2014)*.

O presente estudo considerou um modelo de localização bidimensional (xOy) a partir de 3 (três) receptores que usa o método de Chan para resolver o sistema hiperbólico que indica a posição do transmissor. Os *scripts* utilizados nos testes foram criados a partir do *software* MATLAB.

3 INFLUÊNCIA DA GEOMETRIA DOS RECEPTORES SOBRE A PRECISÃO DA LOCALIZAÇÃO

A acurácia da localização eletrônica por TDOA depende não apenas do algoritmo de localização, mas também do erro na estimação da diferença do tempo de chegada e da geometria entre os receptores e o transmissor (MUÑOZ et al, 2009).

Estudos empregando as propriedades do *Cramer -Rao lowerbound* (CRLB) para otimizar o arranjo de sensores a partir da identificação do tempo de chegada e do ângulo de chegada que

proporcionassem o menor CRLB identificaram que a otimização do arranjo de receptores a partir de uma geometria adequada reduz o erro de localização do transmissor. (CAKIR, 2013).

Na mesma direção, pesquisas sobre o emprego complementar de algoritmos baseados em TDOA a fim de melhorar a acurácia da localização aferida por tempo de chegada do sinal (TOA) identificaram que a posição dos receptores influência a precisão do resultado e que esta apresenta boa acurácia quando submetida a uma geometria adequada (MARTIN-ESCALONA, BARCELO-ARROY, 2008).

O presente trabalho busca identificar quais variáveis da disposição espacial dos receptores influenciam a precisão da localização e qual comportamento elas apresentam, a fim de propor premissas para a otimização do posicionamento do sistema de guerra eletrônica.

Durante uma operação militar, o posicionamento dos receptores considera aspectos técnicos e táticos, possibilitando atingir a configuração adequada para o desempenho dos sistemas com a adequada segurança dos equipamentos e do pessoal envolvido. É utilizado como referência a área de interesse a qual se deseja monitorar, definida como a região espacial que apresenta alta probabilidade da existência de ameaças.

A partir da avaliação preliminar, os receptores são posicionados próximos à área de interesse por meio de distintos arranjos geométricos que apresentam variações de distâncias e ângulo entre os elementos do conjunto.
A falta de informação sobre a influência da geometria do arranjo de receptores sobre a precisão da localização eletrônica poderá ocasionar um posicionamento indevido dos equipamentos de monitoração reduzindo a capacidade do sistema de aferir a posição do alvo.

4 TESTES E RESULTADOS

Foram testados os arranjos de receptores em linha, em cunha, em cunha invertida e circular nos ambientes sem multipercusos e com multipercusos. Utilizou-se o método de Chan para resolver o sistema de localização hiperbólica.

4.1 TESTE EM AMBIENTE SEM MULTIPERCURSO

Nesse primeiro teste foram avaliados a resposta do método de Chan em um cenário sem multipercursos ou ruído, sendo identificados os seguintes resultados:

a) o método de Chan não apresentou nenhuma solução quando os receptores foram posicionados em linha.

b) de acordo com a forma geométrica adotada e a posição do transmissor, o método de Chan apresentará 02 (duas) possíveis soluções. Tal situação demonstra a existência de ambiguidade de resultados, estando alinhado com estudos teóricos sobre a localização por TDOA (COMPAGNONI, 2014). Nesses casos, é necessário um método auxiliar para identificar qual a resposta correta, por exemplo, a direção geral do alvo, obtida por meio de técnicas de Direção de Chegada.

c) o arranjo circular com a área de interesse interna apresentou menor porcentagem de ambiguidade nos resultados, seguido pela disposição em cunha e por último a geometria em cunha invertida, com maior proporção de soluções ambíguas.

4.2 TESTE EM AMBIENTE COM MULTIPERCURSO

Nesse teste foi verificado a relação entre a raiz do erro médio quadrático (RMSE) da localização com as seguintes variáveis espaciais: ângulo de interseção entre as hipérboles, distâncias entre os receptores e ângulos internos do arranjo.

Foram analisadas as geometrias em cunha, em cunha invertida e circular em um cenário com erros provocados por multipercusos, sendo identificadas as seguintes conclusões:

a) o ângulo de interseção entre as hipérboles relaciona-se com a precisão do resultado no arranjo em cunha e circular. Verificou-se que na medida que o ângulo de interseção cresceu monotonicamente, o RMSE da localização decresceu. Tal relação, no entanto, não foi verificada para a disposição em cunha invertida;

b) para a geometria em cunha e circular existem outras variáveis espaciais que influenciam a precisão da localização além do ângulo de interseção;

c) a geometria circular apresentou resultados com alta precisão quando os receptores são dispostos nos vértices de um triângulo equilátero, mantendo o transmissor no centro. Nessa disposição, quanto maior a distância entre os receptores e o transmissor, maior é a precisão da localização;

d) a geometria circular com a disposição equidistantes dos receptores e transmissor no centro apresentou resultados com menor RMSE do que o arranjo em cunha.

4.3 PREMISSAS PARA DISPOSIÇÃO DOS RECEPTORES

Verificou-se que a melhor forma para dispor o sistema de localização por TDOA é a geometria circular com os receptores dispostos sobre os vértices de um triângulo equilátero e o transmissor no centro.

Percebeu-se ainda que para a geometria circular, quanto mais afastados os receptores estiverem do centro da área de interesse menor será o RMSE. Tal configuração garante alta precisão e baixa ambiguidade nos resultados.

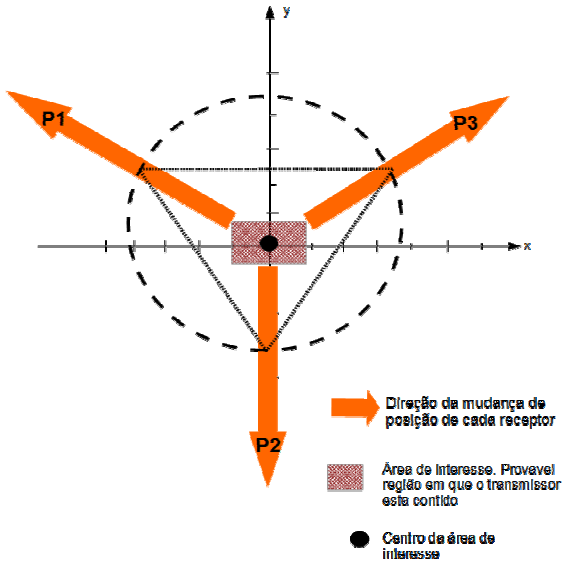
No entanto, devido a limitações decorrentes do tipo de operação militar que inviabilize o uso do arranjo circular, é possível posicionar os sensores na geometria em cunha e atingir resultados com boa precisão, desde que dispostos a partir de relações adequadas.

As geometrias em linha e cunha-invertida, por sua vez, são inadequadas para desdobrar sistemas TDOA devido a dificuldade para o processamento matemático dos dados de entrada.

As informações obtidas complementam a doutrina sobre o assunto, auxiliando o planejamento de guerra eletrônica.

A Figura 1 apresenta os parâmetros a serem considerados para a disposição em geometria circular.

Figura 1—Parâmetros do arranjo circular



Fonte: o autor (2018).

Para aumentar a precisão da localização para disposição circular deve-se observar as seguintes situações:

a) a disposição circular apresenta RMSE menor que a disposição em cunha;

b) o percentual de resultados ambíguos é menor para a geometria circular do que para o arranjo em cunha;

c) área de interesse deve ser posicionada ao centro do círculo formado pelo vértice de um triângulo equilátero;

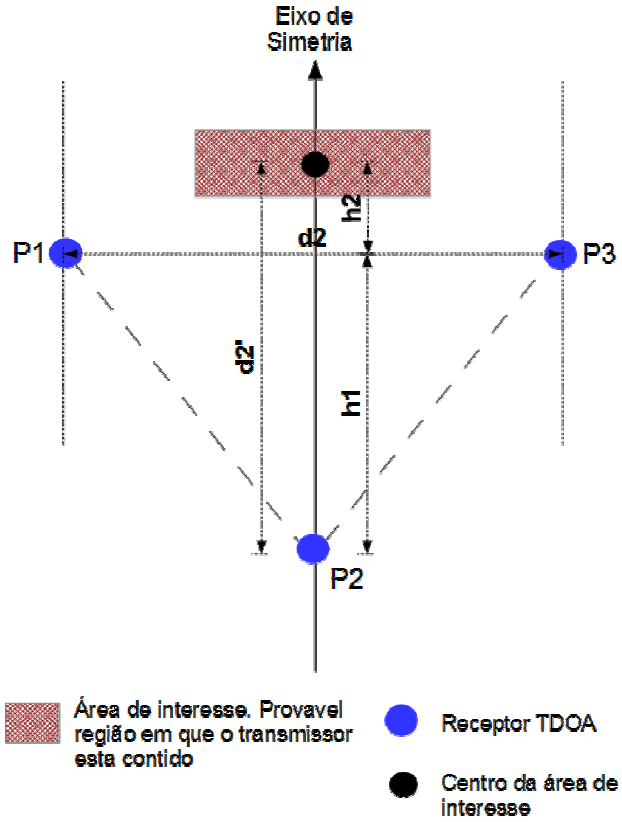
d) a distância do centro da área de interesse até cada receptor deve ser igual;

e) quanto mais afastado os receptores forem posicionados do centro da área de interesse maior será a precisão da localização;

f) existem outras configurações em que os receptores podem ser dispostos na geometria circular que apresentam um RMSE ligeiramente menor do que obtido utilizando a formação circular a partir de um triângulo equilátero, contudo a falta de um padrão de formação inviabiliza a utilização desses outros tipos de configuração.

A **Figura 2** define os principais parâmetros a serem consideradas durante a disposição em cunha.

Figura 2—Parâmetros do arranjo em cunha



Fonte: o autor (2018).

A maior precisão da localização para disposição em cunha é obtida por meio da adequação com as seguintes condições:

a)posicionar o arranjo de forma simétrica, com o receptor central P2 e o centro da área de interesse (região onde encontra-se o transmissor) sobre o eixo de simetria;

b)a área de interesse deve estar contida dentro dos limites definidos pelos receptores das extremidades P1 e P3 a fim de garantir maior ângulo de interseção;

c)maior distância (**d2'**) entre o receptor central P2 e o transmissor para garantir maior comprimento da região correlacionada;

d)maior distância (**d2**) entre os receptores P1 e P3 a fim de proporcionar maior ângulo de interseção entre as hipérboles. Não ultrapassar o limite da região correlacionada;

e)para as posições em que **h1≥h2**, a distância (**d2**) entre P1 e P3 pode atingir o valor máximo de **2x**(**h1+h2),** sem que eles saiam do ponto limite de correlação da linha.

f)posicionar os receptores P1 e P3 mais próximos do transmissor (**menor valor de h2**). Nas simulações foi utilizada a distância mínima de 1 Km;

5 CONCLUSÃO

O presente trabalho analisou a influência da disposição espacial dos receptores de guerra eletrônica baseados em diferença de tempo de chegada (TDOA) sobre a precisão da localização.

A acurácia do resultado de um sistema por TDOA sofre a influência do canal, do erro na estimação do tempo de chegada, do algoritmo de localização e da geometria dos receptores.

Considerando a incapacidade para alterar parâmetros relacionados ao *hardware*, ao algoritmo de localização e ao canal, uma forma alternativa para reduzir o erro de localização seria dispor os receptores em uma determinada geometria que possibilite a máxima precisão do sistema.

Desse modo, esse trabalho buscou identificar variáveis espaciais que apresentem relação com a precisão em um ambiente de multipercurso e modo como se relacionam, a fim de estruturar regras para otimizar a escolha da posição e auxiliar o planejamento de Guerra Eletrônica.

Verificou-se que a melhor forma para dispor o sistema de localização por TDOA é a geometria circular com os receptores dispostos sobre os vértices de um triângulo equilátero e o transmissor no centro, contudo, observou-se que também é possível posicionar os receptores na geometria em cunha e atingir resultados com boa precisão quando dispostos por meio de regras adequadas.

Cabe ressalvar que as conclusões atingidas foram baseadas no método de Chan para solucionar o sistema hiperbólico. Mesmo sendo um método consagrado, não é possível garantir que essas relações sejam mantidas caso o algoritmo de localização seja baseado em outro modelo matemático, cabendo maiores estudos a fim de confirmar se as conclusões apresentadas nesse trabalho podem ser mantidas para outros métodos.

Dessa forma, percebe-se que o tipo de geometria adotada e a escolha das posições, com distâncias e ângulos distintos, possuem grande influência sobre a precisão da localização. Logo, o estudo sobre as relações espaciais que permitem a otimização do posicionamento dos receptores é de grande importância, uma vez que permite reduzir o erro de localização em ambientes com multipercursos, garantindo maior rapidez para identificação e contenção de possíveis ameaças em um cenário militar.
As análises apresentadas complementam as informações doutrinárias sobre o assunto e contribuem para o planejamento de guerra eletrônica a fim de garantir a máxima eficiência do sistema.

REFERÊNCIAS BIBLIOGRÁFICAS

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

COMPAGNONI, Marco; NOTARI, Roberto. TDOA-based localization in two dimensions: the bifurcation curve. ***Fundamenta Informaticae*****,** v. 135, n. 1-2, p. 199-210**,** 2014.

MARTIN-ESCALONA, Israel; BARCELO-ARROY, Francisco. Impact of geometry on the accuracy of the passive-TDOA algorithm. In: Personal, Indoor and Mobile Radio Communications (PIMRC), 2008. IEEE 19th International Symposium. **Proceedings***...* France (Cannes): IEEE, 2008. p. 1-6.

MUÑOZ, David, et al. **Location Techniques and Applications.** Burlington: Elsevier, 2009. 257p.

*Artigo realizado a partir do trabalho de conclusão do Curso de Especialização em Análise de Ambiente Eletromagnético do Instituto Tecnológico de Aeronáutica (CEAAE) em 2015 pelo Capitão de Comunicações Leonardo Possideli Moreira do Exército Brasileiro. Email: leonardo.possideli@eb.mil.br

O uso da ferramenta SDNPWN como forma de Pentest em uma rede definida por software

1º Ten QCO Lamartine de Oliveira Medeiros*

RESUMO

As Redes Definidas por Software (Redes SDN) apresentam características específicas quanto ao fato de segurança e ataques cibernéticos. Com o avanço das tecnologias e arquiteturas de redes, surgiu a necessidade de otimização do monitoramento e controle das redes em camadas dos níveis mais altos do modelo OSI, mais precisamente na camada de aplicação. Com essa nova abordagem surgiu novas formas de ataques cibernéticos testando a vulnerabilidade destas estruturas. No presente trabalho foram abordadas as características das redes SDN, o funcionamento do protocolo OpenFlow. Foram abordadas as principais vulnerabilidades e os problemas de segurança que ocorrem na infraestrutura SDN e quais componentes deste tipo de rede são atacados. Também foram levantados os principais projetos que visam a mitigação dos ataques. Por fim foi utilizado o software MININET para simular uma rede SDN utilizando o protocolo OpenFlow Floodlight e o framework SDNPWN que possui uma série de módulos para reconhecimento, gerenciamento, ataque e exploração de redes SDN. As simulações tiveram por objetivo verificar o comportamento e respostas de uma rede SDN simulada mediante os comandos realizados pelo framework.

Palavras-chave: Redes Definidas por Software. SDNPWN. Openflow.

The use of the SDNPWN tool as a form of attack in a software-defined network

ABSTRACT

Software Defined Networks (SDN Networks) have specific characteristics regarding security and cyber attacks. With the advancement of network technologies and architectures, the need for optimization of the monitoring and control of networks in layers of the highest levels of the OSI model, more precisely at the application layer. With this new approach emerged new forms of cyber attacks testing the vulnerability of these structures. In the present work the characteristics of the SDN networks were discussed, the operation of the OpenFlow protocol. The main vulnerabilities and security issues that occurred in the SDN infrastructure and which components of this type of network are attacked were addressed. The main projects aimed at mitigating attacks have also been raised. Finally, we used the MININET software to simulate an SDN network using the OpenFlow Floodlight protocol and the SDNPWN framework that has a series of modules for the recognition, management, attack and exploitation of SDN networks. The simulations were designed to verify the behavior and responses of a simulated SDN network using the commands performed by the framework.

Keywords: Software Defined Networks. SDNPWN. OpenFlow.

1 INTRODUÇÃO

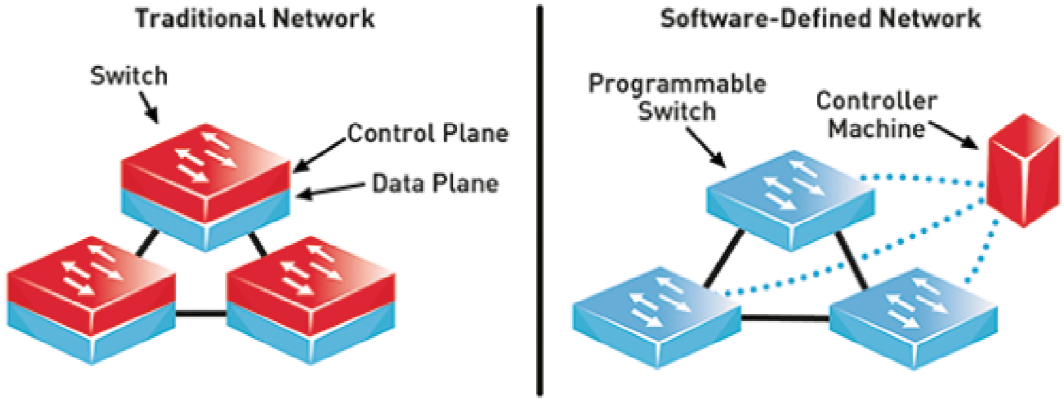
O sucesso das redes, sobretudo da internet é baseado em um princípio de distribuição de protocolos nos roteadores e switches permitindo que os pacotes se movam por toda a parte. Por conta disso o gerenciamento das redes tradicionais é considerada uma tarefa bastante desafiadora, com recursos bastante escassos de mecanismos de resposta e configurações para tarefas automatizadas. Aliado a isto, as redes IP existentes são verticalmente integradas ou seja: o plano de dados que encaminha o tráfego e o plano de controle que faz o encaminhamento são empacotados no mesmo dispositivo, dificultando as pesquisas de inovação, como fica evidenciado na lenta transição do IPv4 para o IPv6 (KREUTZ et al, 2015).

O uso das redes definidas por software (SDN) surge como uma proposta para viabilizar o controle e o gerenciamento das redes, tendo como principal objetivo resolver o problema da inflexibilidade das redes de computadores (GUEDES, 2012). A proposta é que as aplicações na rede: como roteamento inteligente, balanceamento de carga, controle de acesso e qualidade de serviço sejam implementadas para trabalhar em uma aplicação que utilize os recursos do Controlador SDN ao invés de trabalhar em cada roteador ou switch. Pode-se dizer que a rede definida por software é caracterizada pela existência de um sistema de controle, implementado em software, que pode controlar o mecanismo de encaminhamento dos elementos de comutação da rede por uma interface de programação bem definida (GUEDES, 2012).

Desta forma as promessas de agilidade, controle simplificado e programabilidade, que é a possibilidade de ajustar o comportamento de suas redes para oferecer suporte a novos serviços sem se preocupar com restrições de plataformas fechadas ou proprietárias, em tempo real são incentivos para a pesquisa e evolução das redes SDN, mas e quanto a segurança? Quais são as potenciais vulnerabilidades desta nova arquitetura? Quais os pontos frágeis e a mitigação que pode ser realizada?

Por ser uma nova tecnologia, a fragilidade em termos de segurança das SDN é motivo para crescimento de ataques através da descoberta de seus serviços e dispositivos (BOMFIM, 2017).

Figura 1—Rede tradicional e rede definida por software



Fonte: Bonfim (2013).

2 REDES DEFINIDAS POR SOFTWARE (RDS)

As Redes de Computadores foram projetadas e construídas como um conjunto de dispositivos de hardware com propósitos distintos entre si. Estas servem para processar todo o tipo de informação, inclusive o controle da própria rede como o monitoramento de tráfego e roteamento (CENTENO, 2016). Assim as redes vêm se tornando parte de uma infraestrutura crítica, uma vez que essa tecnologia permeia todos os níveis da sociedade, pois sua utilização está nos lares, na forma das redes domésticas, na rotina de implementação de políticas públicas, na forma do governo eletrônico, na educação, onde a internet se tornou uma das fontes essenciais de informação. Por conta disso paradigmas surgiram ao longo do tempo, onde podemos verificar, conforme Nadeau (2013):

a) o poder de processamento focado na evolução dos servidores: por ser mais rentável comercialmente, as pesquisas para o aumento do poder de processamento procuraram focar mais em funcionalidades específicas dos servidores, como por exemplo a execução de aplicativos de servidores de e-mail, servidores de banco de dados e outras funcionalidades que pudessem ser utilizadas pelos usuários;

b) a era da computação elástica: capacidade de aumentar ou reduzir rapidamente os recursos de

armazenamento, memória e processamento para atender às exigências de forma dinâmica. O controle é feito por ferramentas de monitoramento de sistema, denominadas *hypervisor,* que ajustam a quantidade de recursos alocados à quantidade de recursos realmente necessários sem interromper as operações;

c) a virtualização das redes: o conceito das redes virtuais tomou força com as redes virtuais privadas (VPN) possibilitando o isolamento de uma rede de forma segura, isolando totalmente o seu tráfego;

d) os equipamentos de rede: os equipamentos de rede viraram "caixas-pretas", ou seja, implementações integradas baseadas em hardware proprietário (COSTA, 2013). Mesmo com a evolução dos *data centers*, os equipamentos de rede permaneceram parados em termos de inovação, ou seja, além do aumento constante de velocidade na interface, as comunicações de dados não evoluíram muito desde o advento do IP, o *Multi-Protocol Label Switching* (MPLS), que é uma tecnologia de encaminhamento de pacotes, baseada em rótulos, que atua entre as camadas 2 e 3 do modelo *Open System Interconnection* (OSI) e tecnologias móveis (NADEAU, 2013);

e) a calcificação das redes: a estrutura das redes tornou-se calcificada, sendo que todas as pesquisas realizadas, principalmente para a Internet são no nível de aplicação. Neste nível é onde se tem controle e não no núcleo da rede, que seriam as camadas que possuem as funções de transporte e roteamento e se tornaram muito dependentes da tecnologia de fabricantes como CISCO, 3COM entre outros (GUEDES et al, 2012).

Com a proposta das redes SDN surge a possibilidade de uma nova arquitetura de rede capaz de ser programada sob demanda, ou seja, redes programáveis (COSTA, 2013). A SDN propõe a separação do plano de controle e do plano de dados de uma rede fazendo com que a mesma se adapte facilmente às alterações (NADEAU, 2013).

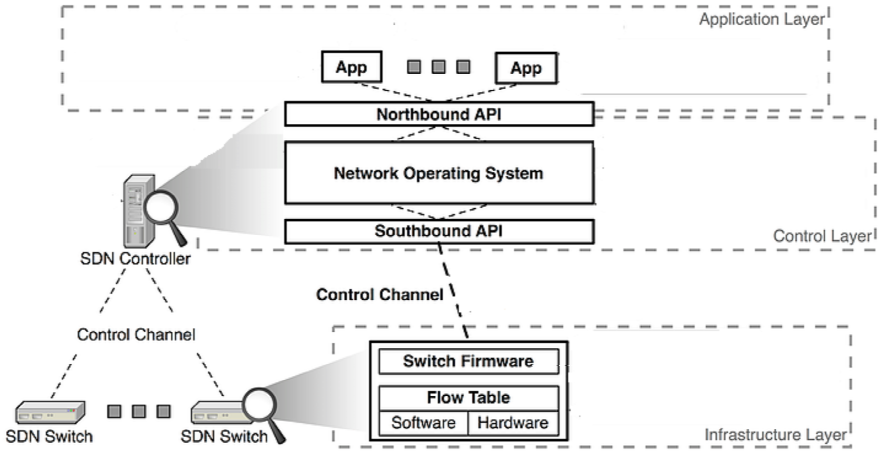
2.1 CARACTERÍSTICAS DAS REDES DEFINIDAS POR SOTFWARE

Em uma rede SDN existem três partes distintas separadas por camadas: aplicação, controlador e plano de dados. A camada de aplicação indica a parte que explora a dissociação do controle e do plano a fim de obter as metas específicas, como mecanismos de segurança ou soluções de gerenciamento de Internet. Esta é a camada em que aplicações e serviços definem o comportamento da rede (BONFIM, 2017).

O plano de dados lida com os pacotes de acordo com as instruções do Controlador. Normalmente, o plano de dados é o ponto final dos serviços do controlador e aplicações, não tendo apenas responsabilidade pelo roteamento ou descarte dos pacotes, mas também possui recursos para realização a classificação dos pacotes (BONFIM, 2017).

O plano de controle (Controlador) é responsável pelos protocolos e pela tomada de decisões que resultam na tabela de encaminhamentos, controlando dessa forma como o plano de dados vai encaminhar seus conteúdos (COSTA, 2013).

Figura 2 -Infraestrutura SDN e principais pontos de ataque



Fonte: SDN SECURITY, (2016) adaptado pelo autor.

A comunicação entre o plano de controle e o plano de dados, ou seja, entre o *controller* e seus dispositivos de rede ocorre através da *Southbound Interface* (SBI). Para que ocorra essa comunicação são necessários 06 itens que o Controlador precisa saber:

a) os dispositivos que estão na rede;

b) o que cada dispositivo é capaz de fazer;

c) quais portas e interfaces que tem o dispositivo;

d) o atual estado de cada porta;

e) topologia;

f) configuração dos dispositivos (BONFIM, 2017).

As alterações necessárias serão realizadas entre as aplicações (APIs) do Controlador através da *Northbound Interface* (NBI). Assim, a SBI coleta as informações, encaminha ao Controlador, que por sua vez passa para a NBI, que coleta essas informações e envia para a API ou aplicações de software que envia de volta instruções para alteração dos pacotes, quando necessário via SBI para o plano de controle dos equipamentos (BONFIM, 2017).

2.2 CONTROLADOR

Em linhas gerais, o Controlador é um sistema de software ou uma coleção de sistemas que juntos proveem:

a) gerenciamento do estado da rede, com informações de configurações, topologia aprendida e informações da sessão de controle;

b) um modelo de dados de alto nível que captura os relacionamentos entre os recursos gerenciados, políticas e outros serviços providos pelo controlador;

c) uma interface de programação de aplicativos (API) moderna com o objetivo de facilitar a interação entre o Controlador e as aplicações;

d) uma sessão segura de controle do *Transmission Control Protocol* (TCP) entre o controlador e os agentes associados nos elementos de rede;

e) um protocolo baseado em padrões para provisionamento de rede orientada a aplicativos de acordo com o estado dos elementos da rede;

f) mecanismo de descoberta de rede, topologia e serviço; um sistema de descoberta de rotas e potencialmente outros serviços centrados na rede ou informações de recursos centrados (NADEAU, 2013);

Para os softwares de *switches*/roteadores o controlador SDN é uma crítica interface de gerenciamento, o qual fornecem serviços de provisionamento e descoberta de redes, sendo responsáveis pelo estado associado das entidades da rede (NADEAU, 2013).

2.3 PROTOCOLO *OPENFLOW*

Originalmente concebido como um protocolo para experimentos acadêmicos, evoluiu a ponto de ser utilizado em substituição aos protocolos de camada 2 e 3 completamente em *switches* comerciais e roteadores (NADEAU, 2013). A proposta do *OpenFlow* promove a criação das redes SDN com a utilização de elementos comuns como *switches* e roteadores, pontos de acesso ou computadores pessoais (COSTA, 2013).

Umas das vantagens de se utilizar a arquitetura *OpenFlow* é a flexibilidade que ela oferece para se programar de forma independente, o tratamento de cada fluxo da rede e como ele dever ser ou não encaminhado. O *OpenFlow* determina como o fluxo dever ser definido, quais serão as ações que podem ser realizadas por pacote do fluxo e quais protocolos de comunicação devem ser utilizados entre o controlador e os comutadores para realizar as definições de fluxo e ação (COSTA, 2013).

3 ASPECTOS DE SEGURANÇA E VULNERABILIDADES DAS REDES SDN

Considerada uma tecnologia recente, a segurança das redes SDN tornou-se uma questão prioritária a ser resolvida, necessitando de um ambiente simples, escalável e eficiente. Como inicialmente, segurança não foi considerado como parte do desenvolvimento das SDN, cada camada possui implicações e requerimentos que necessitam serem avaliadas como questões de segurança. A rede necessita de um *framework* robusto que garanta a direção correta do controlador. Apesar de que a segurança deveria ser construída como parte da arquitetura SDN, ela seria entregue como um serviço para prover privacidade e integridade de todos os recursos conectados (BONFIM, 2017).

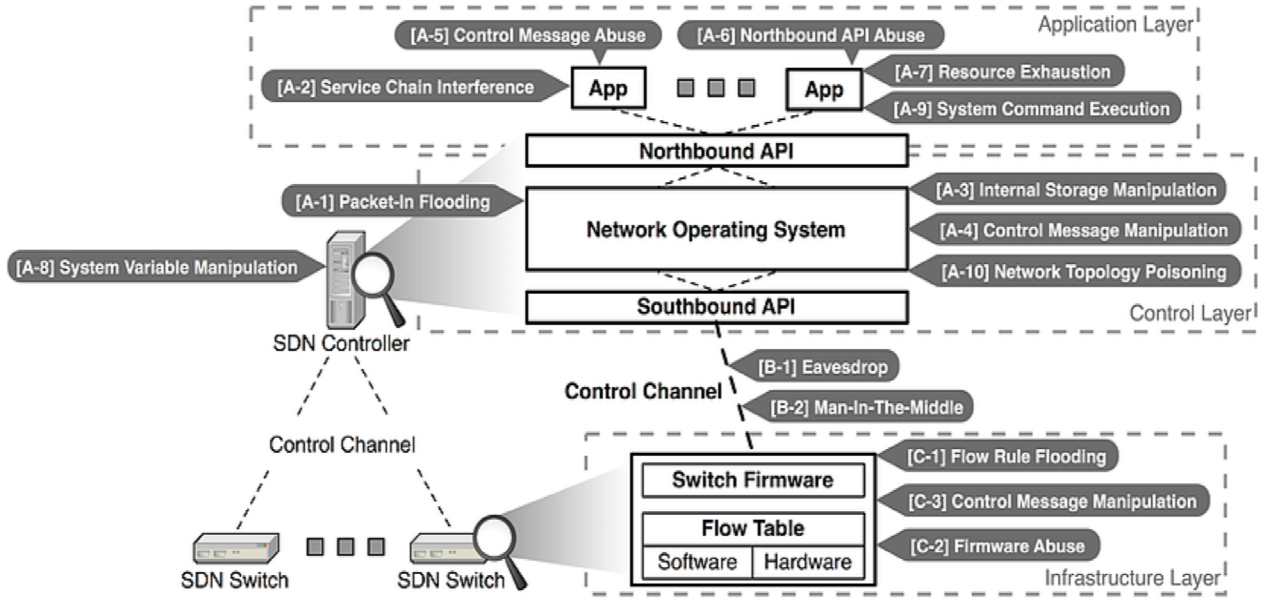
Em 2013 os estudantes Seungwon Shin e Guofei Gu publicaram um artigo sobre segurança em Redes SDN chamado "Atacando redes definidas

por software: uma primeira viabilidade de estudo" (SHIN; GU, 2013) onde realizaram diversos laboratórios com a arquitetura SDN sendo levantados vários problemas de segurança, que segundo os autores não poderiam ser ignorados. O objetivo era dar o ponta pé para diversos estudos na área. Logo após este estudo, ainda em 2013 foram criados os sítios eletrônicos http://www.sdnsecurity.org (SDN SECURITY, 2017) e http:// www.openflowsec.org (OPEN FLOW SEC, 2017) com o objetivo de estimular pesquisadores a divulgarem seus trabalhos sobre segurança em redes SDN. A comunidade do sdnsecurity.org preocupa-se com as falhas de segurança na arquitetura SDN e a comunidade do openflowsec.org é voltada mais para as falhas de segurança no protocolo *OpenFlow* (SDN SECURITY, 2017).

Os colaboradores da comunidade sdnsecurity.org criaram o Projeto GENOMA (SDN SECURITY, 2017) com o objetivo de focar as vulnerabilidades do ambiente de redes SDN, e visa sistematizar ou caracterizar as vulnerabilidades existentes, além disso, encontrar novas vulnerabilidades que não foram relatadas, procurando desenvolver de forma séria, cada vez mais ambientes seguros de redes SDN (SDN SECURITY, 2017). Segundo este estudo os ataques SDN foram divididos em três categorias: a) plano de controle específico: que inclui todos os casos de ataques contra controle SDN e camada de aplicação; b) canal de controle específico: que visam todos os ataques a interface, como por exemplo o *OpenFlow;* e c) plano de dados específico: que estuda os ataques em dispositivos que suportam funções SDN (SDN SECURITY, 2017).

Baseado nisso foram levantados os principais tipos de ataques conforme demonstrado na figura 2, onde são observadas quais ameaças agem dentro da estrutura SDN e quais dispositivos são atacados.

Figura 3 - Infraestrutura SDN com seus principais pontos de ataque e tipos de ataques



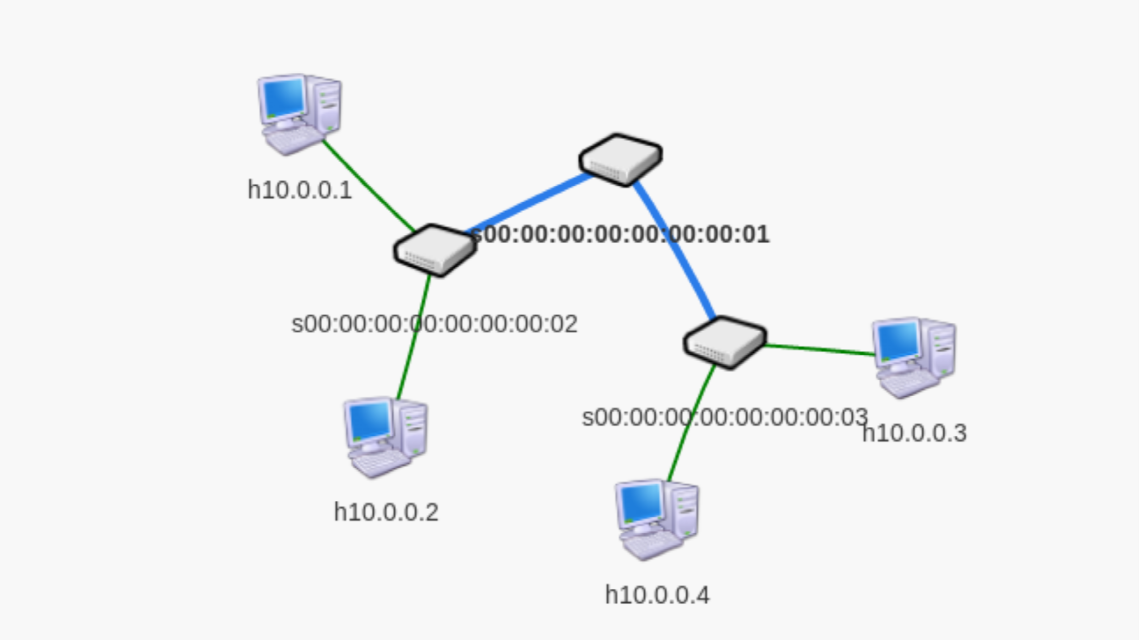
Fonte: SDN Security (2013).

Com o objetivo de mitigar essas vulnerabilidades foram criados uma série de projetos de pesquisa em segurança de redes SDN que são mantidos pelos pesquisadores e colaboradores do sdnsecurity.org.

4 ESTUDO DE CASO

Por serem consideradas estruturas críticas e devido ao alto valor dos equipamentos em ambientes reais, para viabilizar a situação optou -se pela utilização do *MININET* (MININET.ORG, 2017) (www.mininet.org) que é uma ferramenta que permite emular os componentes típicos de uma rede SDN (CENTENO, 2016).

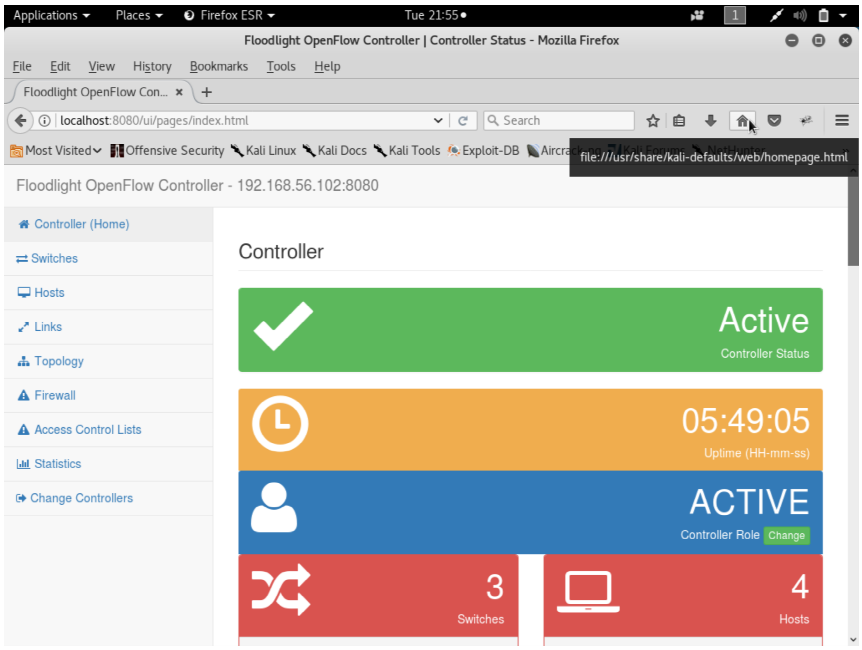
Figura 4 - Topologia da Rede Definida por Software criada pelo MININET



Fonte: o autor (2018).

O simulador *MININET* permite uma rápida simulação de uma grande infraestrutura virtual de rede, executando em um *kernel* real, com a utilização de apenas um computador. O *MININET* cria uma rede virtual *OpenFlow* com um controlador, *switches*, *hosts* e *links,* permitindo também desenvolver topologia personalizadas utilizando *scripts* em *python* (MARCHESAN; MEDINA, 2015). Para a realização dos testes foi utilizado o protocolo *OpenFlow Floodlight*, sendo escolhido por conta do carregamento de módulos extensíveis da linguagem java, como por exemplo o controle via *web* (CENTENO, 2016).

Figura 5 - Módulo web do Controlador Floodlight



Fonte: o autor (2018).

4.1 FERRAMENTA DE TESTE DE PENETRAÇÃO PARA REDES DEFINIDAS POR SOFTWARE

A ferramenta chamada Software Defined Networking Pown (SDNPWN) é um kit de ferramentas de teste de penetração para redes definidas por software (SDN), sendo que possui uma série de módulos a serem utilizados para experimentos e ataques a redes SDN. Pode-se dizer que o SDNPWN é um conjunto de ferramentas que inclui módulos para reconhecimento, outros para ataque e para explorar vulnerabilidades em controladores SDN. Escrito em python 3, o SDNPWN visa habilitar os ataques genéricos de SDN a serem realizados, ao mesmo tempo que permite vulnerabilidades específicas a serem exploradas. O SDNPWN possui 17 módulos; sendo 03 módulos de reconhecimento, 04 módulos de gerenciamento e 10 módulos de ataque e exploração. Cada módulo contém o código usado para uma função específica de ataque ou exploração, com outros módulos atuando como bibliotecas (SMITH, 2016).

4.1.1 Reconhecimento

As capacidades de reconhecimento do sdnpwn estão separadas em três módulos; arpmon, sdn-detect e controller-detect. Todos esses módulos tem o objetivo de identificar os componentes de uma rede SDN. O módulo arpmon pode ser usado para imprimir informações do tráfego ARP capturado em uma determinada interface. O módulo sdn-detect é usado para verificar se uma rede é ou não uma SDN. O módulo controller-detect é usado para identificar o controlador na rede, essa identificação é realizada monitorando o tráfego do protocolo de descoberta de camada de ligação (LLPD), ou enumerando a interface norte do controlador (SMITH, 2016).

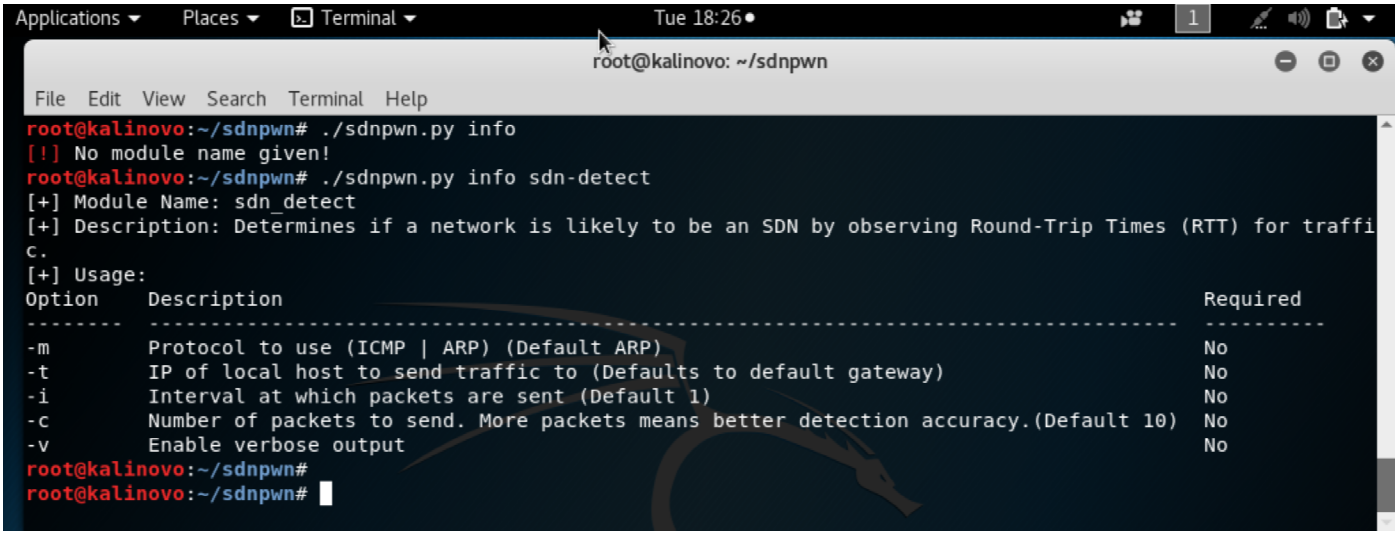
4.1.2 Gerenciamento

Existem quatro módulos de gerenciamento que servem para gerenciar as principais informações sobre a ferramenta e sobre o uso de cada módulo, sendo eles o módulo help que auxilia no uso da ferramenta, o módulo mods lista todos os módulos executáveis que estão na ferramenta, o módulo info mostra a descrição e as opções disponíveis para um módulo específico da ferramenta e o módulo system que é acessado por uma infraestrutura de linguagem comum (Common Languace Infraestructure – CLI), que define um ambiente que permite a utilização de multiplas linguagens de alto nível em diferentes plataformas, mas sem a necessidade de serem reescritas para uma arquitetura específica.

4.1.3 Ataque

Existem ainda os módulos que são utilizados para ataque e exploração de vulnerabilidades da rede SDN e principalmente do controlador SDN. O lfa-relay, lfa-scapy e lldp-replay são usados para executar o Link Fabrication Attack (LFA). O módulo host-location-hijack é usado para executar o sequestro de localização de host. O módulo of-switch é usado para se conectar a um controlador usando o OpenFlow com uma versão de switch personalizada. Isso é útil para reunir padrões de fluxo, testar a segurança do canal de controle e explorar as vulnerabilidades no controlador através da configuração de switch personalizada (SMITH, 2016).

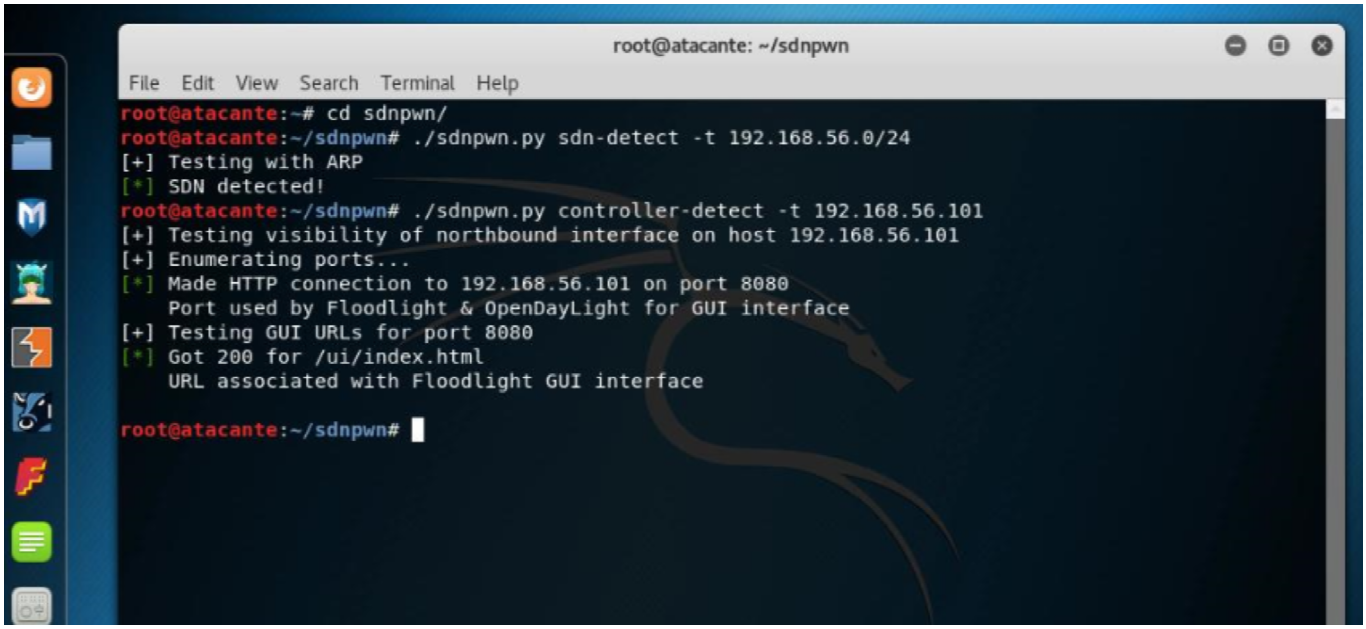
Figura 6 - Exemplo de uso do módulo de informações



Fonte: o autor (2018)

Como exemplo de invasão foi utilizado o módulo of-gen da ferramenta. Através dos parâmetros utilizados com esse módulo foi possivel demonstrar a exploração da vulnerabilidade OpenDayLight CVE-2017-1000357. Esta vulnerabilidade afetou a versão 3.3 do protocolo FloodLight (lítio-SR3), utilizada no teste, onde o invasor que possua acesso ao canal do controlador SDN e desde que o TLS não esteja habilitado para conexões de switch, consegue inundar uma grande quantidade de mensagens do OpenFlow Hello a uma alta taxa, sendo usado o módulo of-gen do SDNPWN. Com esse módulo o controlador SDN de um endereço IP conhecido, na porta 6653 será inundado por pacotes a uma taxa de 1 a .0001 segundos até que 100.000 mensagens tenham sido enviadas (SMITH, 2016). Primeiramente foram realizadas as detecções da rede SDN e do protocolo utilizado.

Figura 7 - Identificando a rede SDN e seu controlador

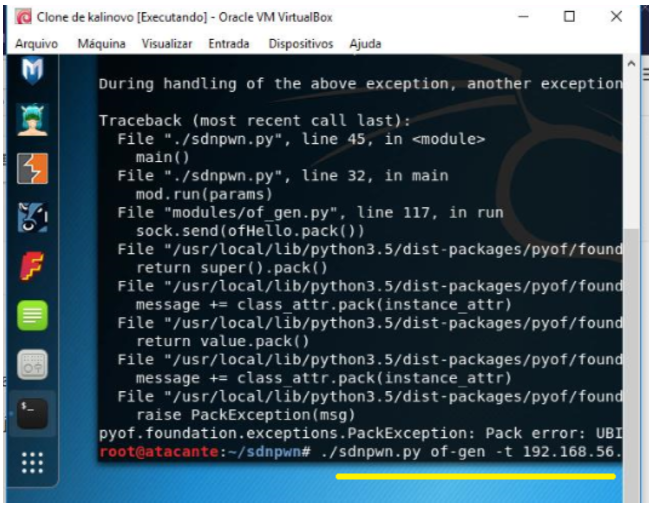


Fonte: o autor (2018)

Logo após utilizando o módulo of-gen realizou-se a inundação de pacotes conforme a Figura 7.

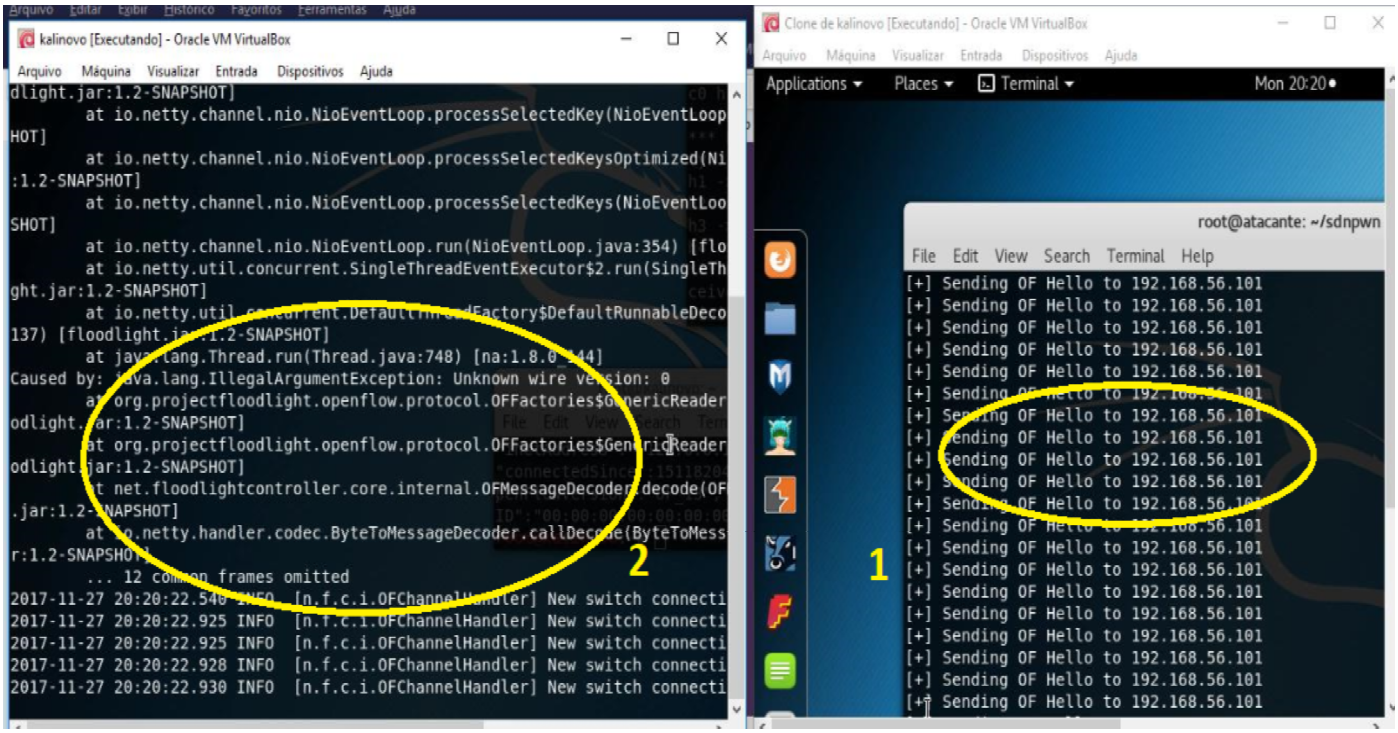
Na Figura 8 verificou-se a dificuldade do controlador tentar restabelecer o serviço e não conseguindo.

Figura 8 - Aplicando o módulo *of-gen*



Fonte: o autor (2018)

Figura 9 - Inundação de pacotes sobre o controlador utilizando o módulo *of-gen*



Fonte: o autor (2018).

E por fim o resultado do ataque utilizando o módulo *of-gen,* conforme figura acima.

A partir da descoberta desta vulnerabilidade foram criados patchs de correção a este problema. Como mitigação do problema recomenda-se que, em caso de uso de uma versão mais antiga, seja a mesma atualizada. (SMITH, 2016).

5 CONCLUSÃO

O presente trabalho buscou apresentar um exemplo de vulnerabilidade e as possíveis falhas de segurança, ressaltando que por ser uma tecnologia recente durante a elaboração do projeto de arquitetura, não houve um cuidado específico referente a segurança das Redes Definidas por Software. Por conta disso, viu-se a necessidade de criação de uma equipe de colaboradores através do SDNSECURITY.ORG, o qual procura criar projetos referentes as vulnerabilidades específicas, procurando resolver os problemas de segurança encontrados.

Através da utilização do simulador SDN MININET juntamente com o controlador Floodlight, foi implementada a utilização do framework SDNPWN.

Este framework foi desenvolvido em python e possui uma série de módulos que possibilitam verificar o reconhecimento, gerenciamento e ataque em redes SDN.

As Redes Definidas por Software por serem uma tecnologia recente, embora tenham a projeção de grandes avanços para o desenvolvimento de novos serviços e soluções, ainda carecem de muitas pesquisas, especialmente na área de segurança.

Caso não seja possível a atualização, a exposição dos serviços OpenFlow do controlador devem ser limitadas a dispositivos confiáveis. Se o OpenFlow não estiver sendo utilizado como um protocolo Southbound, os serviços OpenFlow devem ser desativados (SMITH, 2016).

Por fim, como forma de sugerir novos trabalhos, pode-se citar o desenvolvimento de novos módulos com o objetivo de fazer parte da ferramenta SDNPWN, agregando novos conhecimentos, contribuindo tanto na formação técnica quanto cientifica dos interessados no assunto.

REFERÊNCIAS BIBLIOGRÁFICAS

BOMFIM, Leonardo Henrique da Silva. **Um serviço para anonimização em redes definidas por software.** Sergipe: UFS, 2017. Disponível em < https://bdtd.ufs.br/bitstream/tede/3767/2/LEONARDO_HENRIQUE_SILVA_BOMFIM.pdf >. Acesso em: 31 ago. 2017.

CENTENO, Paulo Vieira. **Uma análise de segurança das redes definidas por software sobre o protocolo OpenFlow**. Florianópolis: UFSC, 2016. Disponível em : < https://repositorio.ufsc.br/bitstream/handle/123456789/171402/monografia_tcc_paulo_centeno.pdf?sequence=1&isAllowed=y > . Acesso em: 3 set. 2017.

COSTA, Lucas Rodrigues. **OpenFlow e o paradigma das redes definidas por software**. Brasília: UNB, 2013. Disponível em < http://bdm.unb.br/handle/10483/5674 >. Acesso em: 31 ago. 2017.

GUEDES, Dorgival et al. **Redes Definidas por Software**: uma abordagem sistêmica para o desenvolvimento de pesquisas em redes de computadores. In: XXX SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS, p. 160-210, 2012. Disponível em: < http://homepages.dcc.ufmg.br/~mmvieira/cc/papers/minicurso-sdn.pdf >. Acesso em: 2 set. 2017.

KREUTZ, Diego et al. Software-defined networking: A comprehensive survey. **Proceedings of the IEEE**. [S.l.]. v. 130, p. 10–76, 2015. Disponível em: < https://pdfs.semanticscholar.org/d8bd/4c1e92420200bd29cb1a233bd81eb3c28bba.pdf >. Acesso em: 2 set. 2017.

MARCHESAN, Gabriel; MEDINA, Roseclea Duarte. **Simulando cenários para redes definidas por software. 2015.** UFSM. Disponível em < http://eati.info/eati/2015/assets/anais/Longos/L20.pdf>. Acesso em: 2 nov. 2017.

MININET.ORG. Disponível em < https://www.mininet.org/>. Acesso em: 7 nov. 2017.

NADEAU, Thomas D.; GRAY, Ken**. SDN:** Software Defined Networks. California. O' Reilly Media, 2013.

OPENFLOWSEC.ORG. Disponível em < https://openflowsec.org/>. Acesso em: 7 nov. 2017. [**SDNSECURITY.ORG**. Disponível em < https://sdnsecurity.org/>. Acesso em: 7 nov. 2017.

SHIN, Seungwon; GU, Guofei. **Attacking Software-Defined Networks**: a first feasibility study. 2013. Disponível em:<http://conferences.sigcomm.org/sigcomm/2013/papers/hotsdn/p165.pdf >. Acesso em: 2 nov. 2017.

SMITH, Dylan. **SDNPWN:** pratical software-defined network security. 2016. [S.l.] Disponível em < https://sdnpwn.net/>. Acesso em: 7 nov. 2017.

*Artigo realizado a partir do trabalho de conclusão do Curso de Especialização em Guerra Cibernética para Oficiais do Centro de Instrução de Guerra Eletrônica (CIGE) em 2017 pelo 1º Tenente Quadro Complementar de Oficiais Lamartine de Oliveira Medeiros do Exército Brasileiro. Email: lamartine.medeiros@eb.mil.br

Aplicação operacional da RF em fotônica: o enlace analógico a fibra óptica e a faixa dinâmica livre de espúrios

Cap Com Bruno Elias Ribeiro*

RESUMO

Os primeiros sistemas a empregarem a tecnologia de radiofrequência (RF) em fotônica datam da década de 90. Desde então, diversas melhorias foram implementadas em sistemas de RF que utilizam dispositivos fotônicos, estejam estes dispositivos empregados em conjunto ou em substituição a dispositivos eletrônicos. Os dispositivos fotônicos têm sido empregados em Enlaces Analógicos a Fibra Óptica (EAFO) tendo em vista aplicações comerciais civis ou de interesse militar. Neste sentido, uma das características a estudar é a faixa dinâmica livre de espúrios (SFDR – Spurious Free Dynamic Range), que delimita, por exemplo, a sensibilidade e o ponto de operação, sem distorções de um radar ou de um sistema de guerra eletrônica. Também são abordadas neste artigo algumas vantagens dos EAFO, já que eles asseguram maior eficiência aos sistemas de RF a eles associados, dado o emprego de dispositivos fotônicos. Prevê-se que os sistemas vocacionados para emprego militar que utilizem estes dispositivos estarão comercialmente disponíveis em um futuro bem próximo, compondo sistemas de armas e sistemas de guerra eletrônica, dadas as imposições dos cenários de combate e as perspectivas de evolução para as tecnologias de RF em Fotônica.

Palavras-chave: Radiofrequência. Fotônica. Enlace analógico a Fibra Óptica.

Operational application of Microwave Photonics: *the Analog Photonic Link and the Spurious Free Dynamic Range*

ABSTRACT

The The first devices to deploy Microwave Photonics technologies date from the nineties. Since then, several improvements have been made in radiofrequency (RF) systems which use photonic devices, deployed along or replacing electronic devices. Photonic devices have been used in Analog Photonic Links (APL) seeking commercial civilian applications or applications that are interesting to the military. This way, one feature to be studied is the Spurious Free Dynamic Range (SFDR), which limits, for instance, sensibility and distortion-free operation of a radar or an electronic warfare system. This article also points at APLs advantages, since they provide higher efficiency to associated RF systems, once photonic devices are used there. It is foreseen that military systems deploying these devices will be commercially available in the near future, inside weapons systems and electronic warfare systems, given the requirements of battlefield scenarios and the evolutions predicted to microwave photonics technologies.

Keywords: *Radiofrequency. Microwave Photonics. Analog Photonic Link.*

1 INTRODUÇÃO

No dia 6 de agosto de 1960, Theodore Maiman publicou na revista Nature os resultados obtidos ao irradiar um cristal de rubi de 1 cm com uma lâmpada de flash de alta potência (MAIMAN, 1960). Este experimento formalizou a invenção do laser de estado sólido. A partir daí, com o amadurecimento desta tecnologia, a luz amplificada pela emissão estimulada de radiação (LASER – Light Amplification by Stimulated Emission of Radiation) se mostrou uma invenção muito útil para diversas aplicações, em especial para as comunicações ópticas (KEISER, 2014).

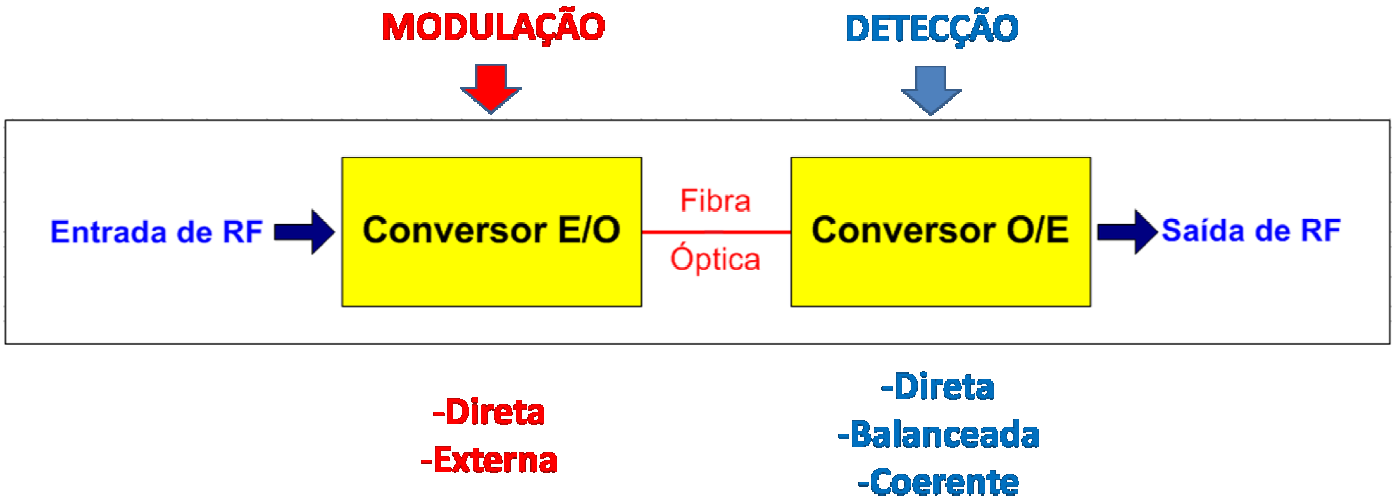
Uma das primeiras aplicações comerciais neste sentido foi a utilização de fibras ópticas para a transmissão de sinais de TV a cabo.

Outra aplicação, de interesse militar e não relacionada a comunicações, foi a transmissão de sinais de radar por fibra óptica a partir de uma estação controladora afastada a dezenas de quilômetros da antena do radar (COX III, 2004).

As aplicações supracitadas são possíveis devido ao emprego do laser em um EAFO. Nesta arquitetura, o sinal de RF a ser transmitido a longas distâncias modula a portadora no espectro

de frequências ópticas gerada pelo laser. Este sinal modulado é transmitido por fibra óptica até um fotodetector ou um conjunto de fotodetectores responsável por converter o sinal transmitido do espectro de frequências ópticas para o espectro de frequências de RF (COX III, 2004).

Figura 1 - Diagrama esquemático de EAFO para a transmissão de sinais de RF.



Fonte: o autor (2018).

A Figura 1 apresenta um diagrama esquemático de um EAFO, ressaltando as possibilidades para a modulação e a detecção do sinal de RF. O sinal de RF, na conversão do espectro de frequências elétrico para óptico (E/O), modula uma portadora óptica sem o auxílio de um modulador – modulação direta – ou com o auxílio de um modulador – modulação externa, empregando, por exemplo, um modulador de eletroabsorção ou um modulador eletroóptico de intensidade.

O sinal modulado, após sua transmissão por um trecho de fibra óptica, é convertido do espectro de frequência óptica para elétrica (O/E) por meio de detecção direta, balanceada ou coerente, empregando, respectivamente, um fotodetector, mais de um fotodetector, ou técnicas de processamento homódinas ou heteródinas (COX III, 2004).

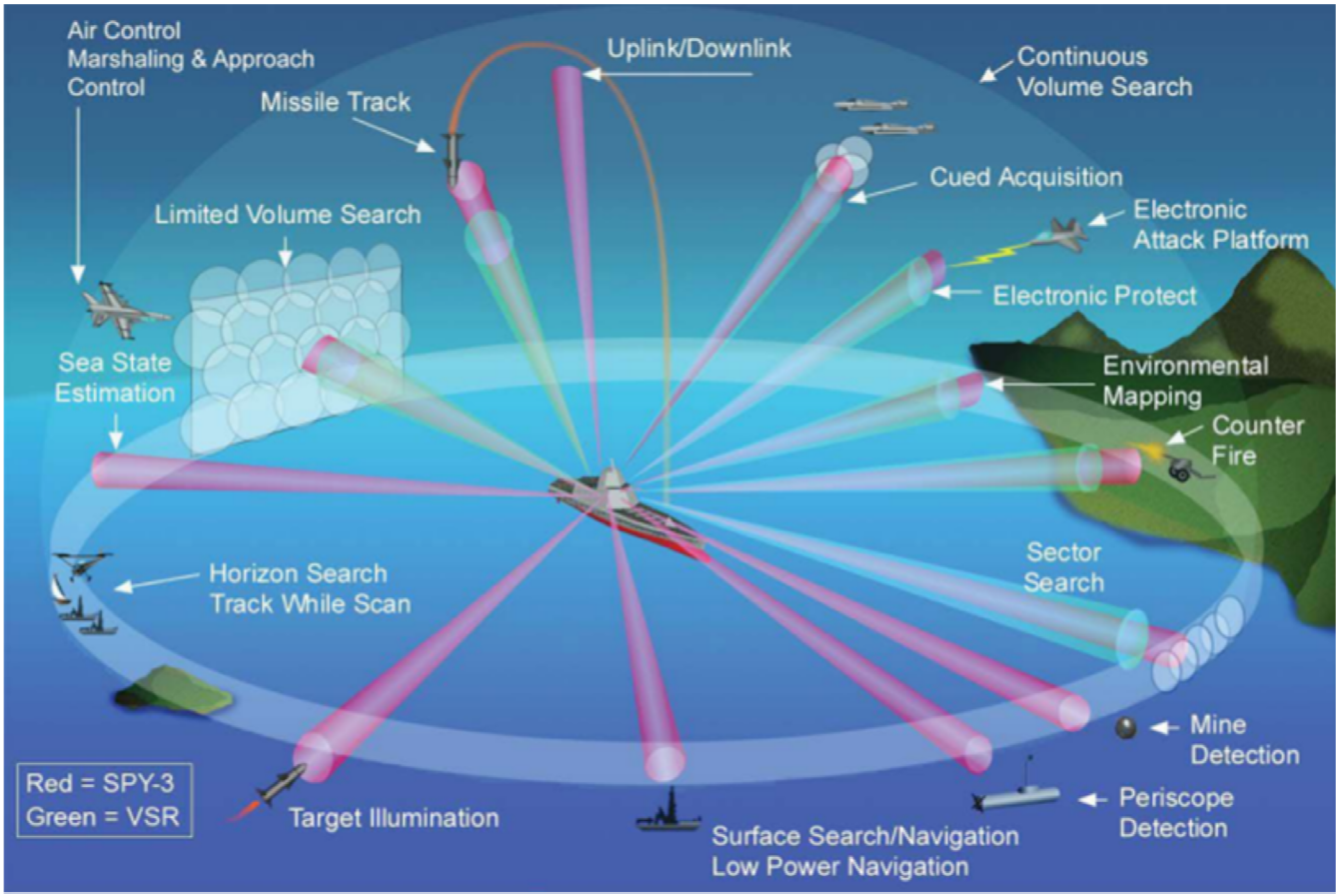
Em 2014, a revista *Nature* trouxe outra publicação de inovação tecnológica de interesse para a defesa, tendo em vista sua aplicação em sistemas de armas, colimada com as necessidades dos cenários de combate modernos: o radar fotônico (GHELFI, 2014).

O radar fotônico, que emprega dispositivos fotônicos para a geração da forma de onda, processamento do sinal de RF e detecção de um ou mais sinais de interesse – proposta dos dispositivos multifuncionais (RIDWAY, 2014; MELO et al, 2016) traz como uma de suas principais vantagens o aumento da largura de banda, proporcionada pelo processamento dos sinais na faixa do espectro óptico.

A Figura 2 ilustra os desafios para a autoproteção de uma plataforma de combate naval. Neste contexto, propõe-se um dispositivo radar multifuncional, capaz de operar em faixas diferentes do espectro eletromagnético – expressas pelos feixes nas cores verde e vermelha – necessitando de grande largura de banda instantânea para a detecção e identificação das diversas ameaças presentes no cenário. Este dispostivo multifuncional da Figura 2 é um exemplo de aplicação possível para o emprego do radar fotônico.

No Brasil, estudos sobre a tecnologia de RF em Fotônica aplicada à defesa são conduzidos por institutos de renome, como o Instituto Nacional de Telecomunicações (INATEL) (MELO et al, 2016) e o Instituto Tecnológico de Aeronáutica (ITA) (COUTINHO, 2018). Nestes institutos, é possível medir, por meio de experimentos práticos, as vantagens obtidas com o uso de dispositivos fotônicos.

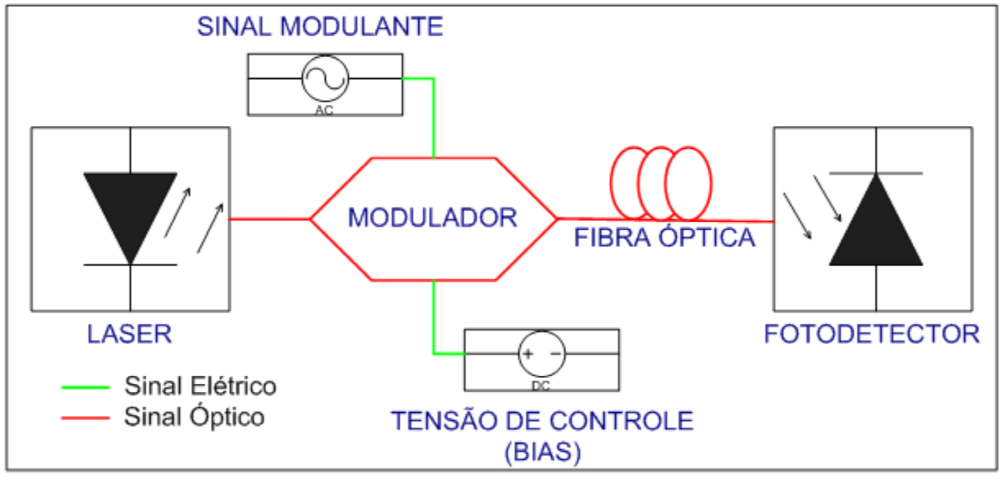
Figura 2 - Desafios da consciência situacional no cenário de combate moderno



Fonte: Bogoni (2018).

Serão apresentadas a seguir algumas figuras de mérito em sistemas de não comunicações e guerra eletrônica (GE), como é o caso da faixa dinâmica livre de espúrios (SFDR – *Spurious Free Dynamic Range*) ou, simplesmente, faixa dinâmica. Ela está diretamente relacionada à detecção de alvos de interesse para sistemas de armas ou de guerra eletrônica, e é apresentada neste artigo no contexto do EAFO. Ainda no contexto da área de pesquisa em RF em Fotônica, conhecida internacionalmente como *Microwave Photonics*, serão exploradas algumas vantagens angariadas com a geração, o processamento e a detecção fotônicos dos sinais de RF. (CAPMANY, NOVAK, 2007).

Figura 3 - Exemplo de EAFO com IMDD para a transmissão de um sinal radar.



Fonte: o autor (2018).

2 O ENLACE ANALÓGICO A FIBRA ÓPTICA

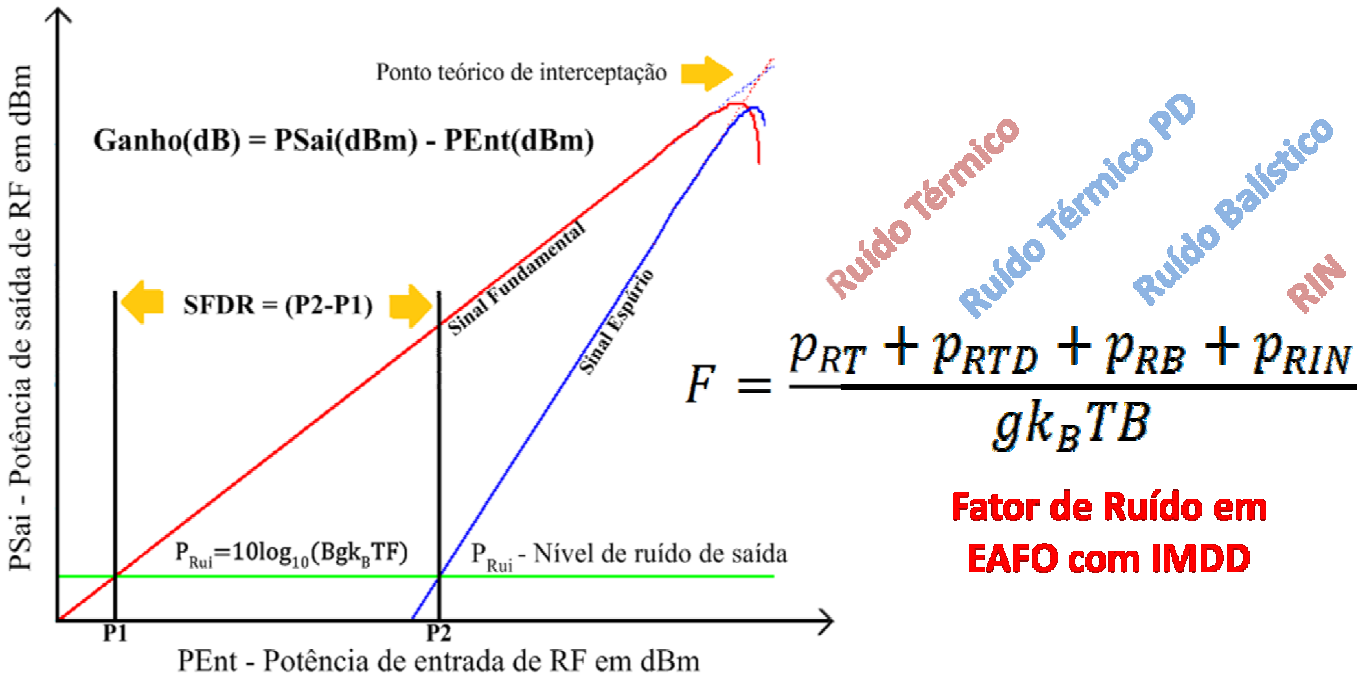
No exemplo da Figura 3, um laser de material semicondutor gera uma portadora óptica na faixa de frequência de centenas de THz. Esta portadora é modulada por um sinal de corrente alternada (AC – *Alternate Current*) na faixa de dezenas de GHz com o auxílio de um modulador eletroóptico de intensidade do tipo Mach-Zehnder (MZM – *Mach-Zehnder Modulator*), caracterizando assim a modulação externa. O ponto ótimo de operação deste modulador é controlado por uma tensão de corrente contínua (DC – *Direct Current*), que regula um valor de potência de transmitância do sinal modulado a ser transmitido pela fibra óptica. Após a sua transmissão, o sinal é fotodetectado a partir da potência óptica incidente no fotodiodo, dispositivo mais comumente empregado neste tipo de enlace, possibilitando a recuperação do sinal AC que modulara previamente a portadora óptica, caracterizando assim o processo de detecção direta.

Traduzindo o parágrafo anterior para o exemplo de uma possível aplicação operacional de um EAFO, pode-se citar a estrutura que permite a operação remota de um radar em relação a sua antena. Esta estrutura abrange o laser que gera a portadora óptica e o MZM, junto com seu controle DC e o gerador AC do sinal de RF.

O processo de modulação ocorre nesta estrutura, e o sinal modulado é transmitido por fibra óptica por dezenas de quilômetros até o fotodiodo, onde ocorrerá a fotodetecção do sinal óptico modulado, a recuperação do sinal de RF e a posterior radiação deste sinal pela antena do radar. O ciclo se repete para o envio do sinal de RF com a informação do alvo detectado pelo radar para a estrutura remota, de forma que a posição onde ocorre a operação do radar também disponha de um fotodetector e estruturas para o pós-processamento do sinal de RF, de forma a executá-lo em posição afastada da antena, garantindo assim a segurança dos operadores e analistas.

Neste tipo de enlace, algumas figuras-de-mérito são de interesse, tendo em vista a correta detecção do alvo por parte de um radar, para empregar o mesmo exemplo. Dentre elas, é possível citar: ganho de RF; fator de ruído; e faixa dinâmica livre de espúrios. Esta última, como será visto a seguir, é decisiva para a correta detecção de alvos e, consequentemente, garantia de êxito na obtenção da consciência situacional em combate. A SFDR e outras figuras -de-mérito serão detalhadas a seguir, e podem ser deduzidas a partir da observação do gráfico da Figura 4.

Figua 4- Figuras-de-mérito de um EAFO com IMDD



Fonte: Ribeiro (2016).

No gráfico da Figura 4, é possível analisar as figuras de mérito de um EAFO com IMDD. O eixo das abscissas corresponde ao valor em dBm da potência do sinal de RF à entrada do EAFO, no processo de modulação (PEnt). O eixo das ordenadas corresponde ao valor em dBm da potência do sinal de RF à saída do EAFO, após a fotodetecção (PSai). Para obter o ganho do EAFO, correspondente à primeira figura-de-mérito de interesse, basta obter o resultado de (PSai - PEnt) referente a qualquer ponto sobre a curva que denota o sinal fundamental, representado na cor vermelha.

A segunda figura-de-mérito de interesse é o fator de ruído do EAFO, que está relacionado ao nível de potência de ruído deste enlace. A potência de ruído é decisiva para o cálculo da SFDR, tendo em vista que ela denota o nível de potência a partir do qual o sinal fundamental, em vermelho, e o sinal espúrio, em azul, são detectados na faixa de passagem do EAFO.

O fator de ruído, dado pela letra F, é proporcional ao ruído térmico, ao ruído balístico e ao ruído de intensidade relativa (RIN – *Relative Intensity Noise*). O ruído térmico está associado ao movimento aleatório de portadores de carga em condutores; o ruído balístico está ligado ao processo estatístico de geração de corrente elétrica em fotodetectores – eventos independentes e randômicos associados à incidência de fótons e geração de portadores livres para a corrente elétrica; o RIN, por sua vez, relaciona-se à corrente de bombeamento do laser e aos processos de emissão espontânea e estimulada associados à geração do laser, resultando em processos randômicos que provocam flutuações aleatórias na potência óptica. (COX III, 2006; 2004).

Obtém-se, assim, a linha verde paralela ao eixo das abscissas, que estabelece o threshold do sistema de detecção.

É possível, então, definir a figura-de-mérito SFDR, calculada no gráfico da Figura 4 pela diferença entre os valores P1 e P2. Estes valores se referem, respectivamente, à potência do sinal fundamental de RF e à potência do sinal espúrio de RF decorrente da distorção.

Na medida em que aumenta a potência do sinal fundamental na entrada do sistema, aqui definido como o alvo de interesse para o radar associado a um sistema de armas, este sinal deve transpor o nível de potência de ruído, ou nível de *threshold*, para ser detectado. O valor P1 indica o nível de potência em que o sinal fundamental transpõe o limiar de ruído e permite sua identificação como alvo, correspondendo portanto ao valor em dBm para a sensibilidade do radar.

No entanto, na medida em que se aumenta o ganho deste sistema de RF, com o aumento dos valores de potência de RF de entrada, o sistema se torna suscetível a distorções. O valor P2 indica o nível de potência em que o sinal espúrio transcende o limiar de ruído e se apresenta na faixa de passagem observada, correspondendo ao alvo falso apresentado ao operador do radar e, portanto, ao valor em dBm limite para a operação deste radar sem distorções. O resultado obtido de (P2 – P1) expressa assim a SFDR ou faixa dinâmica deste radar.

Cabe aqui ressaltar que, apesar de utilizado para estudar o exemplo de um EAFO com IMDD, o gráfico da Figura 4 pode ser empregado para analisar o funcionamento de qualquer sistema que emprega RF, uma vez que os eixos coordenados estão em função dos valores de potência em dBm de entrada e saída dos sinais de RF.

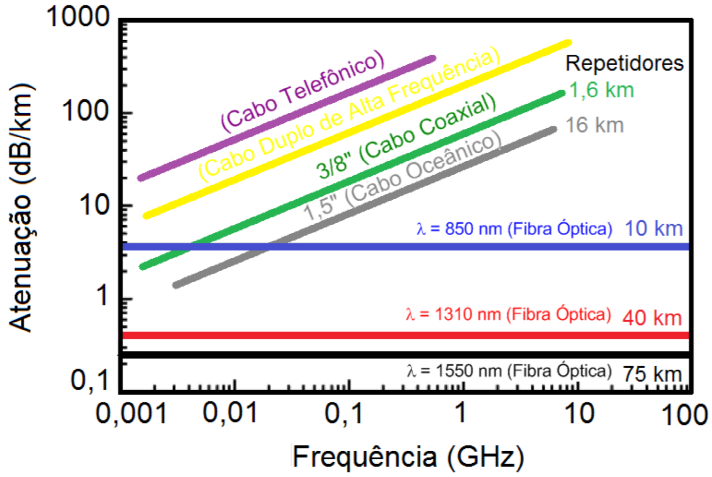
A influência dos dispositivos fotônicos, neste caso, está na lei de formação do limiar de ruído, onde estão presentes a influência do RIN, na geração do laser; e a influência do ruído balístico, no processo de fotodetecção. A influência do ruído térmico está associada aos dispositivos eletrônicos, presentes nas resistências ôhmicas associadas ao modulador (gerador de sinal AC) e ao fotodetector (recuperação do sinal AC que modulara a portadora óptica). Verifica-se, assim, a importância atribuída ao cálculo da figura-de-mérito SFDR para o funcionamento de sistemas de interesse para a guerra eletrônica de não comunicações.

3 VANTAGENS ASSOCIADAS AO EMPREGO DE EAFO

No exemplo apresentado na sessão anterior, optou-se pela fibra óptica para a transmissão do sinal modulado. Contudo, é possível fazer a opção por um sistema que utilize a transmissão do sinal óptico modulado empregando óptica no espaço livre (FSO – *Free Space Optics*). Neste caso específico, deve-se atentar para o alinhamento entre os sensores transmissor e receptor, bem como às características atmosféricas da região do enlace, já que o sinal óptico a ser transmitido é suscetível a absorção, espalhamentlo e turbulências por conta da presença de partículas de poeira e gotículas de água (SANTOS, 2008).

No caso em estudo neste artigo, retomando exemplo do radar, quando a opção é a utilização de cabeamento para a transmissão de sinais de RF, verifica-se que o emprego da fibra óptica é mais vantajoso que o emprego de um cabo coaxial, por exemplo. No exemplo da Figura 3, o sinal de RF a ser transmitido pelo radar – que pode ser gerado por técnicas fotônicas – modula a portadora óptica. A partir daí, o sinal modulado está pronto para ser transmitido pela fibra. Existem três opções janelas de transmissão a empregar, associadas aos comprimentos de onda de 850 nm, 1310 nm e 1550 nm, que oferecem, conforme a Figura 5, suas peculiaridades para a transmissão do sinal modulado. (DIAS, 2017).

Figura 5 - Comparação entre atenuações em diversos meios de transmissão

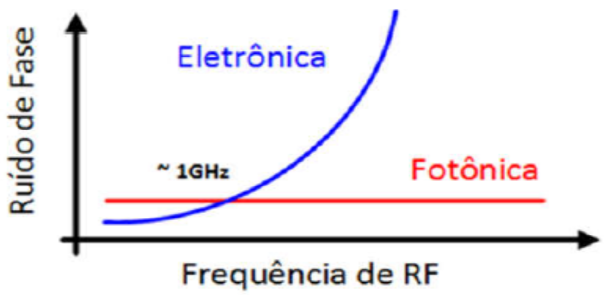


Fonte: COX III (2004) adaptado pelo autor.

A partir da Figura 5 verifica-se que, para transmissão a longas distâncias, independente do comprimento de onda utilizado para a propagação do laser pela fibra óptica, verifica-se que a opção por este meio é mais vantajosa que a que utiliza, por exemplo, um cabo coaxial para transmitir um sinal de RF de 10 GHz. Além da tendência de aumento da atenuação em dB/km com o aumento da frequência, o valor de atenuação para esta frequência é superior quando se emprega cabo coaxial. Ressalta-se ainda a necessidade de repetir o sinal de RF a cada 1,6 km com o uso do mesmo cabo, ao invés de repetir a cada 40 km, com o emprego da fibra óptica no comprimento de onda de 1310 nm. Contudo, conforme o artigo publicado em 2014 pela *Defense Advanced Research Projects Agency* (DARPA), os receptores multifuncionais a serem empregados nos cenários de combate futuros tendem a operar em frequências de operação ainda maiores. No caso do artigo, frequências superiores a 18 GHz e larguras de banda instantâneas superiores a 1 GHz (RIDGWAY, 2014).

Esta tendência vai ao encontro do desejável aumento da largura de banda nestes sistemas de RF de interesse. A operação dos EAFO, a partir da utilização de dispositivos fotônicos em conjunto com dispositivos eletrônicos, possibilita um aumento natural da largura de banda, já que o processamento do sinal pode ocorrer na faixa de frequências do espectro óptico.

Figura 6 - Aumento do ruído de fase em função do aumento da frequência de operação com o emprego de dispositivos eletrônicos (azul) e dispositivos fotônicos (vermelho)



Fonte: Dias (2017).

O aumento da frequência de RF baseada em sistemas que operam apenas com eletrônica convencional traz os seguintes inconvenientes: aumento da complexidade destes sistemas, pelo acréscimo de componentes eletrônicos; aumento da inserção de ruído, dificultando a detecção do sinal fundamental; aumento do peso destes sistemas, restringindo seu emprego em vetores aéreos como os sistemas de aeronaves remotamente pilotadas (SARP) e sistemas satelitais; aumento do custo de desenvolvimento e manutenção; e aumento do consumo de potência para o processamento dos sinais de interesse. O uso dos dispositivos fotônicos apresentados na Figura 3, além de contar com as vantagens proporcionadas pela transmissão por fibra óptica, garante, por sua vez, imunidade a interferências eletromagnéticas, aumenta a largura de banda e reduz o peso e a complexidade dos sistemas.

Estas vantagens estimulam o estudo destas tecnologias, tendo em vista seu emprego em aplicações operacionais de interesse para a defesa. O primeiro exemplo é o radar fotônico italiano, criado a partir do Projeto *Photonic Based Fully Digital Radar System* (PHODIR), que permite a geração, o processamento e a detecção do sinal de RF com o emprego de fotônica (BOGONI, 2013) Pode-se citar ainda o Projeto *Active Phased Array Radio Photonics* (ROFAR), da Rússia, relacionado ao uso de dispositivos fotônicos para gerar o padrão de irradiação de antenas de arranjo de fase (PAA – *Phased Array Antenna*) (THAI Militay…, 2016).

No Brasil, o INATEL fez recentemente o teste de campo de um receptor multifuncional, em parceria com os pesquisadores do radar fotônico. O sistema de uso dual proposto utiliza dispositivos fotônicos, fazendo com que um transceptor se comporte simultaneamente como um radar e como um dispositivo de comunicações, utilizando um único elemento irradiador de RF sem, contudo, prejudicar o seu desempenho global. Utiliza, portanto, uma antena e um transceptor para as duas aplicações: radar e comunicações, o que se reflete em redução de custo, tamanho, peso e consumo de potência pelo sistema (MELO, 2016).

Ainda no Brasil, a pesquisa na área de RF em Fotônica no Instituto Tecnológico de Aeronáutica, aplicada à defesa nacional, segue na mesma direção, com trabalhos acerca da geração fotônica de sinais de RF e do uso de filtros e linhas de retardo fotônicos para emprego em antenas PAA . Esta pesquisa, no âmbito da Força Aérea Brasileira, teve início com a publicação em 1999 do artigo *Trends in Photonics Applied to Electronic Warfare at Brazilian Airforce*, um dos primeiros associados ao surgimento do Programa de Pós Graduação em Aplicações Operacionais (PPGAO) daquela Força Singular, ativo até a presente data e contribuindo com a formação de massa crítica no contexto de tecnologia aplicada à Defesa Nacional. (DIAS, 2017; SILVA, 2017; OLIVEIRA, 1999)

Por tudo isso, verifica-se a atribuição de grande importância às tecnologias de RF em Fotônica, tanto em pesquisas internacionais como nacionais, dadas as vantagens proporcionadas pelo emprego de dispositivos fotônicos em conjunto ou em substituição a dispositivos eletrônicos (MARQUES, 2017). Os sistemas de armas ou sistemas de guerra eletrônica serão mais eficientes com o emprego das tecnologias de RF em Fotônica, dotados de novas capacidades para a aquisição da consciência situacional em combate, com a possibilidade de emprego em plataformas aéreas ou satelitais (BOGONI, 2013).

Para tanto, são perspectivas futuras para o emprego desta tecnologia a miniaturização de componentes, utilizando as tecnologias de fotônica em silício e outros materiais avançados, como o grafeno, para a implementação em uma placa de circuito (*in-chip*) (BOGONI, 2013). Este esforço permitirá o emprego da tecnologia de RF em Fotônica embarcada em SARP e sistemas satelitais, dada a redução do peso, das dimensões e do consumo de potência necessários à operação dos futuros sensores de não comunicações.

4 CONCLUSÃO

Buscou-se apresentar neste artigo a aplicabilidade das tecnologias de RF em Fotônica em cenários de combate futuros, onde o desafio é assegurar a consciência situacional em um ambiente eletromagneticamente denso.

Verificou-se, inicialmente, como funciona um EAFO e quais as principais figuras-de-mérito associadas ao seu funcionamento efetivo. O ganho, o fator de ruído e a SFDR auxiliam a compreender não apenas o funcionamento dos EAFO, mas também de qualquer sistema que utilize RF. Afinal, o EAFO continua a ser uma estrutura para a transmissão e o processamento do sinal de RF, aproveitando as vantagens proporcionadas pela geração, processamento e detecção no espectro de frequências ópticas.

Destas vantagens, foram ressaltadas a baixa atenuação na transmissão do sinal de RF com o emprego da fibra óptica, o aumento da largura de banda instantânea, a redução no peso e nas

dimensões dos sistemas que empregam RF em Fotônica e, consequentemente, menor inserção de ruído pela adoção de componentes e menor consumo de potência. Estas caracterísiticas se mostram promissoras para a implementação *in-chip* destes dispositivos fotônicos, possibilitando a miniaturização de componentes e sua posterior aplicação em SARP e em sistemas satelitais. São capacidades de relevância para agregar aos futuros sistemas de armas e de guerra eletrônica, dados os desafios proporcionados pelos cenários de combate futuros.

Por fim, cabe aqui ressaltar a importância dos instrumentos de parceria no contexto de pesquisa e aplicação da tecnologia de RF em Fotônica, a exemplo do que ocorreu, conforme citado anteriormente, com o INATEL e os pesquisadores do radar fotônico italiano. A pesquisa em RF em Fotônica se mostra relevante para o cenário de defesa, e é importante buscar o conhecimento já disponível junto aos institutos nacionais de renome (Instituto Militar de Engenharia, ITA, INATEL) para consolidar sua aplicação nas capacidades operativas de interesse para as Comunicações e, por conseguinte, para o Exército Brasileiro.

REFERÊNCIAS BIBLIOGRÁFICAS

BOGONI, Antonella. **Phodir project:** photonic based fully digital radar system. CNIT, TECIP, [2013?]. Disponível em: <http:// www.phodir.eu/phodir/file/presentation.pdf>. Acesso em: 3 jun. 2018.

CAPMANY, J.; NOVAK, D. Microwave photonics combines two worlds. **Nature Photonics**, Nature Publishing Group, v. 1, p. 319–330, June 2007.

COUTINHO, O. L. RF em Fotônica e suas aplicações em defesa. Brazil Cyber Defence Summit & Expo – Conferência de Simulação e Tecnologia Militar. **Proceedings...** 2018. Brasília – DF.

COX III, C. H. **Analog Optical Links:** theory and practice. Nova York: Cambridge University Press, 2004. 288 p.

COX III, C. H. et al. Limits on the performance of RF-over-fiber links and their impact on device design. **IEEE Transactions on Microwave Theory and Techniques**, v. 54, n. 2, p. 906–920, Feb. 2006.

DIAS, P. E. S. **Estudo do Ruído de Fase na Geração Fotônica de Sinais de RF**: modelagem e caracterização. 2017. 194 f. Dissertação (Mestrado em Microondas e Optoeletrônica) – Instituto Tecnológico de Aeronáutica, São José dos Campos, 2017.

GHELFI, P. et al. A fully photonics-based coherent radar system. Research Letter. **Nature**, v. 507, p. 341–345, Mar. 2014.

KEISER, G. **Comunicações por fibras ópticas**. Porto Alegre: AMGH Editora Ltda, 2014. 659 p.

MAIMAN, T. H. Stimulated Optical Radiation in Ruby. **Nature**, v. 187, p. 494, Aug. 1960.

MELO, S. et al. Dual-use System Combining Simultaneous Active Radar & Communication, Based on a Single Photonics-Assisted Transceiver. In:INTERNATIONAL RADIO SYMPOSIUM – IRS, 17., 2016. **Proceedings...** [S.l.], 2016.

OLIVEIRA, J. E. B.; ALVES, F. D. P.; MATTEI, A. L. P. Trends in photonics applied to electronic warfare at Brazilian Air Force. In: SBMO/IEEE MTT-S IMOC MICROWAVE OPTOELETRONIC CONFERENCE, 2., 1999, Rio de Janeiro. **Proceedings...** Psicataway: IEEE, 1999, p. 599 –602.

RIDGWAY, R. W. et al. Microwave photonics programs at DARPA. **Journal of Lightwave Technology**, v. 32, n. 20, p. 3428-3439, Oct. 2014.

SANTOS, L. B. **Análise de Sistemas de Comunicação Utilizando Óptica no Espaço Livre**. 2008. 133 f. Dissertação (Mestrado em Engenharia Elétrica) – Instituto Militar de Engenharia, Rio de Janeiro. Disponível em: <http://www.pgee.ime.eb.br/pdf/ leandro_santos.pdf>. Acesso em: 31 jul. 2018.

SILVA, J. L. B. **Filtros e linhas de retardo fotônicos integrados aplicados a sistemas de RF em Fotônica**. 2017. 144 f. Dissertação (Mestrado em Ciências e Tecnologias Espaciais) – Instituto Tecnológico de Aeronáutica, São José dos Campos, 2017.

THAI Military and Asian Region - **Zhuk-AE/FGA -35 modified radar with AESA (ROFAR)**. Disponível em: <https:// thaimilitaryandasianregion.wordpress.com/2016 /03/14/kret-creates-a-laboratory-forresearch-in-photonics/>. Acesso em: 31 jul. 2018.

MARQUES, R. B. et al. Perspectivas de modernização em guerra eletrônica: aplicação militar da fotônica. **Spectrum**, v. 1, n. 20, p. 32 –38, set. 2017.

*Artigo realizado a partir do trabalho de conclusão do Programa de Pós-Graduação em Aplicações Operacionais (PPGAO) do Instituto Tecnológico de Aeronáutica (ITA) em 2016 pelo Capitão de Comunicações Bruno Elias Ribeiro do Exército Brasileiro.Email: eliasribeiro@eb.mil.br.

Funcionalidade dos Software e Hardware livres na Localização De Sinais: estudo de caso, analisando o uso do SDR-RTL pelo método TDOA.

(CT) Pedro Tebaldi Medeiros da Silva*

RESUMO

O Sistema SDR-RTL tem sido cada vez mais explorado no campo da localização de sinais. O sistema apresentou como desvantagem a necessidade de posicionamento do sinal pretendido. Em situações onde o emissor encontrava-se situado fora do triângulo formado pelos receptores, não foi possível obter sua localização precisa; na melhor hipótese, obteve-se a direção do sinal, porém sem um ponto específico para sua posição. Apesar disso, apresentou relevantes vantagens que levaram à conclusão pela sua viabilidade de emprego. Além do baixo custo e fácil acesso, o processamento do sistema se dá no meio digital, não dependendo, assim, da precisão de componentes analógicos do rádio convencional. Foi verificado que o sistema pode ser instalado em ambientes internos sem perder sua eficácia, não sendo necessário locais como campo aberto ou terraços de prédios para seu bom funcionamento. Outra vantagem é a interface do sistema, que facilita tanto sua operação como manutenção, além do amplo número de entusiastas que compartilham informações e algorítimos em diversos sites pela internet. Neste trabalho, verificou-se que os testes realizados se mostraram eficientes e capazes de serem aplicados não apenas no meio civil, mas também pelas Forças Armadas, com a vantagem de custo reduzido e menor emprego de pessoal.

Palavras-chave: Localização de sinais. TDOA. Software livre.

Functionality of Free Software and Hardware in Signal Location: a case study, analyzing the use of SDR-RTL by the TDOA method.

ABSTRACT

The SDR-RTL System has been increasingly explored in the field of signal localization. The disadvantage of the system was the need to position the desired signal. In situations where the emitter was located outside the triangle formed by the receivers, it was not possible to obtain its precise location; in the best case, the direction of the signal was obtained, but without a specific point for its position. Despite this, it presented significant advantages that led to the conclusion of its viability of employment. In addition to low cost and easy access, the processing of the system occurs in the digital medium, thus not depending on the accuracy of analogical components of the conventional radio. It was verified that the system can be installed indoors without losing its effectiveness, and it is not necessary to have places such as open fields or terraces of buildings for their proper functioning. Another advantage is the system interface, which facilitates both its operation and maintenance, as well as the large number of enthusiasts who share information and algorithms on various websites over the internet. In this work, it was verified that the tests performed were efficient and capable of being applied not only in the civilian medium, but also by the Armed Forces, with the advantage of reduced cost and lower personnel employment.

Keywords: *Signal localization. TDOA. Free software.*

1 INTRODUÇÃO

De acordo com Exército Brasileiro (2019), a Guerra Eletrônica compreende o conjunto de ações que tem por finalidade desenvolver e assegurar a capacidade de emprego eficiente das emissões eletromagnéticas próprias, ao mesmo tempo em que buscam impedir, dificultar ou tirar proveito das emissões inimigas.

Poucos podem ter real acesso às atividades de GE, pois os conhecimentos dos seus domínios envolvem tecnologias, técnicas e táticas que têm sido circunscritas a duas categorias limitadas de pessoas: os engenheiros e técnicos peritos no assunto; e os especialistas das forças que planejam o emprego das atividades de GE, operam e executam a manutenção dos seus complexos meios.

Conforme Exército Brasileiro (2019), a GE se divide em dois campos de atuação: Comunicações e Não Comunicações, sendo aquela o foco do presente trabalho.

2 GUERRA ELETRÔNICA

Segundo Adamy (2001), "Guerra eletrônica é definida como a arte e ciência de preservar o uso do espectro eletromagnético para uso amigável, enquanto negando o seu uso para o inimigo.". (ADAMY, 2001, p. 3).

Outra definição pode ser obtida de acordo os ensinamentos de Oliveira (2002): A GE é o componente do emprego militar da eletrônica que abrange ações realizadas com a finalidade de evitar ou reduzir o uso eficaz da energia eletromagnética, radiada pelas forças inimigas, bem como as atividades efetuadas com o propósito de garantir o seu emprego pelas forças inimigas. (OLIVEIRA, 2002, p. 47).

2.1 LOCALIZAÇÃO DE SINAIS

A localização de sinais (ou Localização Eletrônica) pode ser vista como uma das diversas finalidades da GE. De acordo com Exército (2019), "Consiste na determinação, por intermédio de sistemas eletrônicos especializados, da posição geográfica provável de um emissor de energia eletromagnética." (EXÉRCITO, 2019, p. 3-3).

Ainda de acordo com Exército Brasileiro (2019), a precisão da localização de um sinal eletrônico depende, dentre outros fatores, da técnica empregada. Neste trabalho, focaremos o estudo na técnica TDoA – *Time difference of arrival*, a ser abordada em tópico posterior.

3 EQUIPAMENTOS UTILIZADOS NA LOCALIZAÇÃO DE SINAIS

Neste tópico, serão apresentados os equipamentos que serão objeto de estudo do trabalho.

3.1 RÁDIO DEFINIDO POR SOFTWARE (SDR)

De acordo com CHEN e HO (2017), O SDR teve seu início no início da década de 90, quando o Departamento de Defesa dos EUA, visando a atender às demandas por comunicações seguras, iniciou o programa SPEAKeasy com a finalidade de facilitar a integração entre os sistemas de comunicação de rádio. (REED, 2002 apud CHEN, Wen Tzu e HO, Chen-Hsun, 2017).

A fim de definir o que vem a ser o SDR, *Wireless Innovation Forum (2018)* traz a seguinte consideração:

O SDR define uma coleção de tecnologias de hardware e software em que algumas ou todas as funções operacionais do rádio (também conhecidas como processamento da camada física) são implementadas por meio de software ou firmware modificável que operam em tecnologias de processamento programáveis. (WIRELESS, 2018.).

De acordo com Martins (2015), "O conceito de rádio definido por software (SDR) permite substituir a tradicional implementação dos dispositivos de comunicação analógicos por uma implementação mais flexível.". Em sua obra, Martins (2015) afirma que o sistema possui maior flexibilidade de reconfiguração, se comparado aos rádios convencionais, podendo, assim, melhor atender às necessidades de cada operação.

Na mesma obra, SRUTHI (2013) afirma que a tecnologia SDR visa a substituir os *hardwares* de rádio convencionais com a implementação daquele sistema, através de softwares abertos, reconfiguráveis e reprogramáveis.

3.2 RTL-SDR

De acordo com STEWART (2015), o RTL-SDR é um pequeno dispositivo USB compacto e fácil de usar, capaz de receber sinais de rádio RF. Em seu artigo, afirma que o dispositivo possuía outra finalidade quando da sua criação: Originalmente, esses dispositivos foram projetados para uso como DVB-T (*digital vídeo broadcast – terrestrial*) [...], permitindo que os consumidores recebessem transmissão UHF e assistissem TV em seus computadores. (STEWART et al., 2015, p. 65).

Conforme RTL-SDR.COM, O RTL-SDR é um dispositivo USB de baixo custo (aproximadamente US$ 25), que pode ser usado como um *scanner* de rádio baseado em computador para receber sinais de rádio ao vivo. (ABOUT RTL-SDR, 2018).

3.3 O SOFTWARE

A fim de integrar a plataforma do RTL-SDR com o computador, será necessário um *software* para tal. Nesse estudo, foi utilizado o MATLAB. Segundo Stewart (2017): O MATLAB e o Simulink fornecem um ambiente onde você pode codificar e construir os receptores de forma conveniente, e essas caixas de ferramentas fornecerão os meios necessários para

implementar qualquer algoritmo de receptor SDR desejado. Eles não apenas fornecem as facilidades para projetar coisas como os filtros digitais, decimadores e sincronizadores que seu sistema requer, mas também fornecem ferramentas que permitem visualizar sinais nos domínios de tempo e frequência à medida que passam pelo processo de demodulação. (STEWART et al., 2017, p. 6).

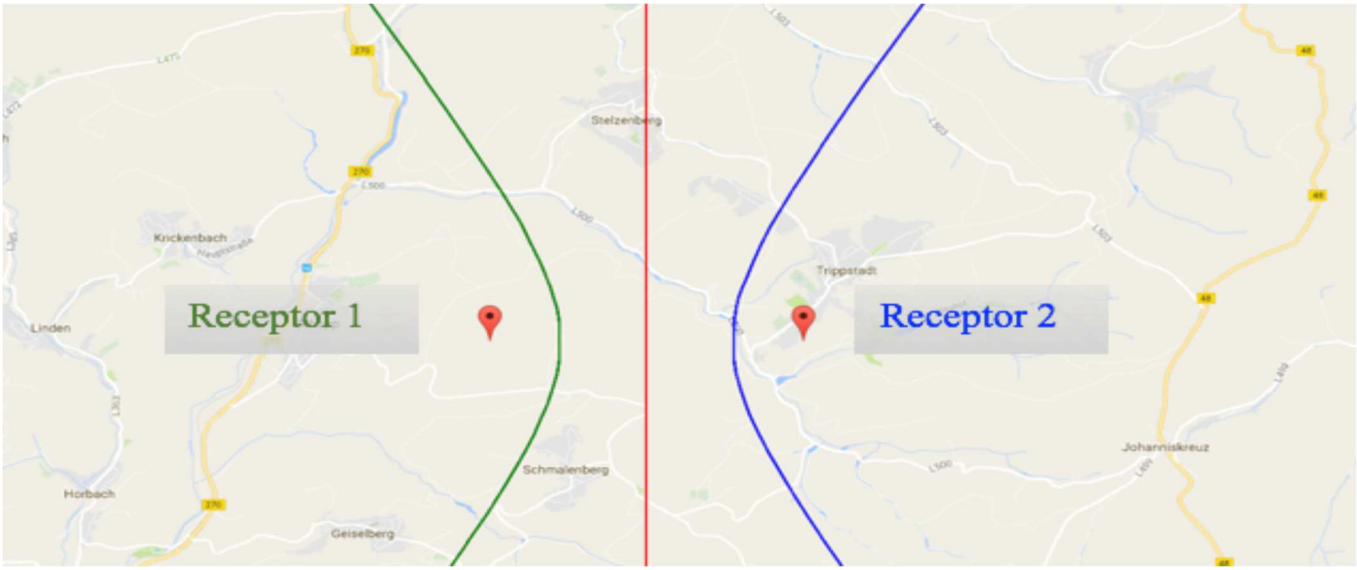
4 ESTUDO DE CASO ANALISANDO O USO DO RTL-SDR

Para o referido estudo, será exposto o experimento realizado por Stefan Scholl em 2017 na cidade de Kaiserslautern, Alemanha.

Inicialmente, Scholl utilizou o que chamou de "situação simplificada", com apenas 2 receptores a fim de localizar a emissão do sinal pretendido. Para tal, utilizou a técnica *Time Difference of Arrival* (TDoA), que Adamy (2001) explica: Um sinal que sai do transmissor em algum momento definido chegará ao receptor no tempo *d/c* mais tarde, onde d é a distância do transmissor ao receptor e c a velocidade da luz. Assim, o tempo de chegada define a distância. Os receptores GPS emitem referências de tempo muito precisas, tornando a medição TOA de precisão muito mais fácil (logisticamente) do que há alguns anos atrás. (ADAMY, 2001, p. 172).

Inicialmente, ilustrou o possível resultado de um teste utilizando apenas dois receptores.

Figura 1 – Situação simplificada com 2 receptores



Fonte: Scholl (2017).

Acima, tem-se 3 hipérboles. A hipérbole central (de cor vermelha) foi obtida após verificar um TDOA de 0ns, ou seja, não houve diferença entre o tempo de chegada do sinal em relação aos receptores. Com isso, observou-se que o emissor poderia assumir qualquer posição ao longo dessa linha, estando, assim, posicionado de forma equidistante dos dois receptores.

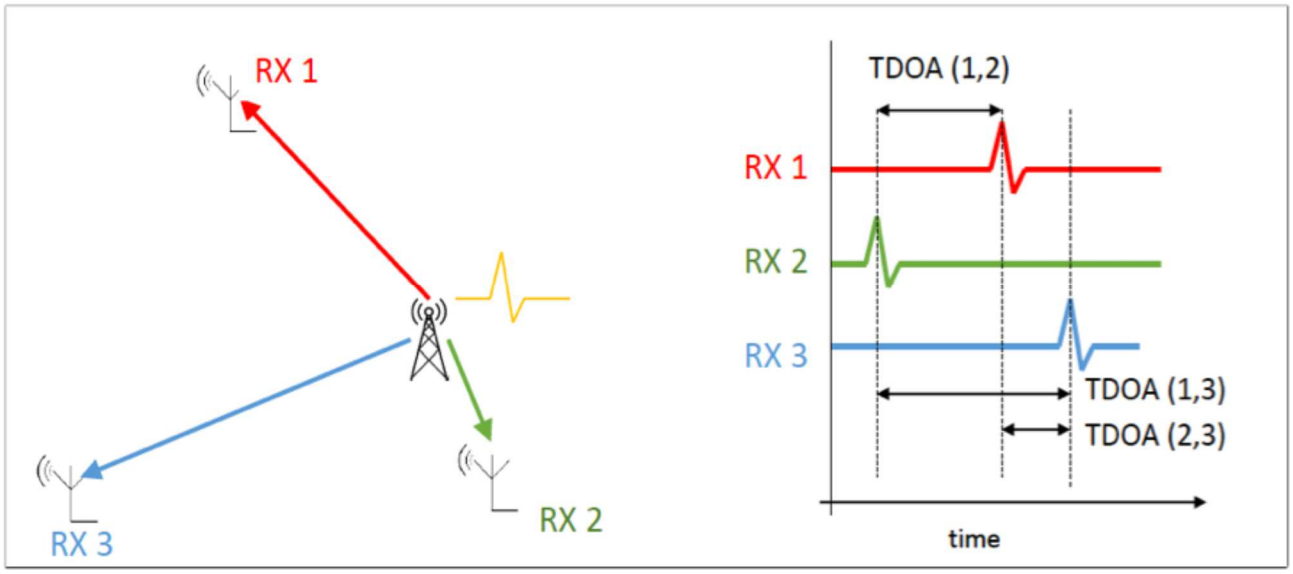
A hipérbole verde foi obtida após verificar um TDOA de 6,7ns entre os receptores. Com isso, concluiu-se que o transmissor estava posicionado 2000m mais próximo do receptor 1 em relação ao receptor 2. Analogamente ao ocorrido com a hipérbole central, o emissor poderia assumir qualquer posição ao longo da hipérbole verde.

Quanto à hipérbole azul, foi obtida após verificar também um TDOA de 6,7ns entre os receptores, porém, agora o emissor estaria localizado mais próximo ao receptor 2, mantendo a mesma relação de distância anterior (2000m).

Assim, concluiu-se que, utilizando apenas 2 receptores, não seria possível precisar a localização da fonte de sinal. Para eliminar as ambiguidades quanto ao posicionamento do emissor, seria necessário acrescentar mais um receptor.

Scholl (2017) ilustrou o que viria a ser a localização pela técnica TDOA utilizando 3 receptores conforme abaixo:

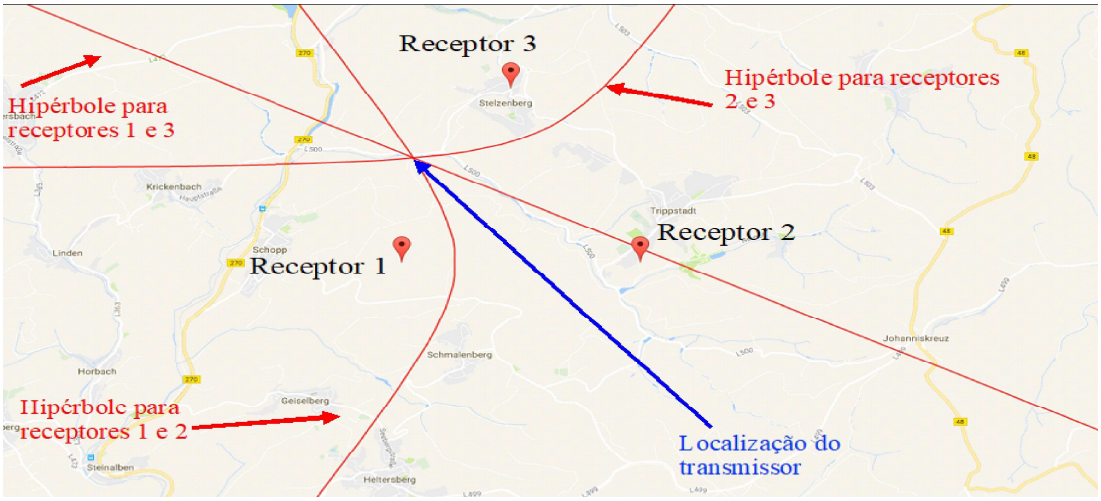
Figura 2 – Técnica TDOA



Fonte: Scholl (2017).

Em seguida, explicou o resultado que seria obtido utilizando 3 receptores dispostos em geometria triangular. Desta forma, a ambiguidade quanto à localização do emissor seria mitigada pelo cruzamento das 3 hipérboles, obtendo, assim, sua localização neste ponto.

Figura 3 – Sistema completo com 3 receptores



Fonte: Scholl (2017).

4.1 CORRELAÇÃO ENTRE OS SINAIS RECEBIDOS

Para calcular o atraso do recebimento dos sinais entre os receptores, Scholl utilizou a seguinte função de correlação:

$$Corr(\tau) = \sum_{t=0}^{N-1} s_1(t)s_2(t+\tau)$$

A correlação é máxima quando os dois sinais casam melhor. Se os dois sinais forem idênticos, esse máximo se dará quando as duas cópias estiverem sincronizadas (sem atraso). (ABU-RGHEFF, 2018, p. 40).

Onde s1(t) e s2(t) são os sinais recebidos pelos receptores 1 e 2.

De acordo com Abu-Rgheff (2007), a correlação é amplamente utilizada para estimar o tempo de atraso e sincronização entre sinais. Segundo o autor: Correlação é a medida de similaridade entre dois sinais quando um está defasado em relação ao outro. A correlação é máxima quando os dois sinais casam melhor. Se os dois sinais forem idênticos, esse máximo se dará quando as duas cópias estiverem sincronizadas (sem atraso). (ABU-RGHEFF, 2018, p. 40).

4.2 POSICIONAMENTO DOS RECEPTORES

Scholl(2017) verificou que, para uma melhor acurácia, o emissor do sinal deveria estar entre os 3 receptores. Em uma situação ideal, os receptores formariam os vértices de um triângulo, e o emissor estaria localizado no no interior deste. Na situação em estudo, não foi possível realizar tal disposição por questões geográficas, visto que seria necessário dispor os receptores em regiões de floresta, com difícil acesso e sinal de internet desfavorável. A figura abaixo ilustra a situação descrita.

Figura 4 - Posicionamento dos receptores

Fonte: Scholl (2017).

4.3 INFRAESTRUTURA DO SISTEMA

A estrutura utilizada por Scholl consiste em 3 receptores RTL-SDR, cada qual ligado a um computador, conectados via internet a um computador mestre.

Assim, o computador mestre é capaz de iniciar a recepção pelos receptores como um "gatilho". Com isso, os receptores recebem o sinal e o transmitem de volta para o computador mestre.

Figura 5 - Infraestrutura do sistema

Fonte: Scholl (2017).

4.4 SINCRONIZAÇÃO

Segundo Scholl (2017), a sincronização é de vital importância para a eficiência do sistema e requer uma precisão na casa dos nano segundos. Para tal, utilizou como referência uma torre de transmissão de sinal áudio digital (de posição conhecida), medindo 120m de altura e uma potência de 2Kw. Segundo Scholl, tais características foram fundamentais para a correlação de sinais.

Figura 6 - Receptores e antena para sincronização

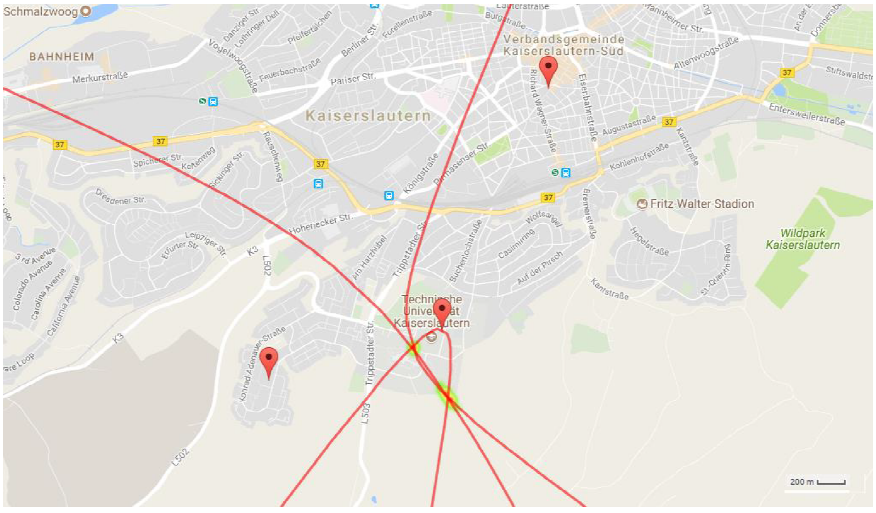
Fonte: Scholl (2017).

5 ANÁLISE DOS RESULTADOS

Nesse tópico, serão demonstrados os resultados obtidos por Scholl em seus testes a fim de se obter a localização dos transmissores de sinal, utilizando um sistema com 3 RTL-SDR conectados via internet a um computador mestre, conforme descrito anteriormente.

O primeiro teste foi realizado tendo como alvo uma antena repetidora de sinal DMR (Rádio Móvel Digital) de 70cm, localizada no topo do prédio da Universidade de Kaiserslautern, a qual operava na frequência de 439,4 MHz, com uma largura de banda de 12,5 KHz e modulação 4-FSK.

Figura 7 - Resultado para antena DMR

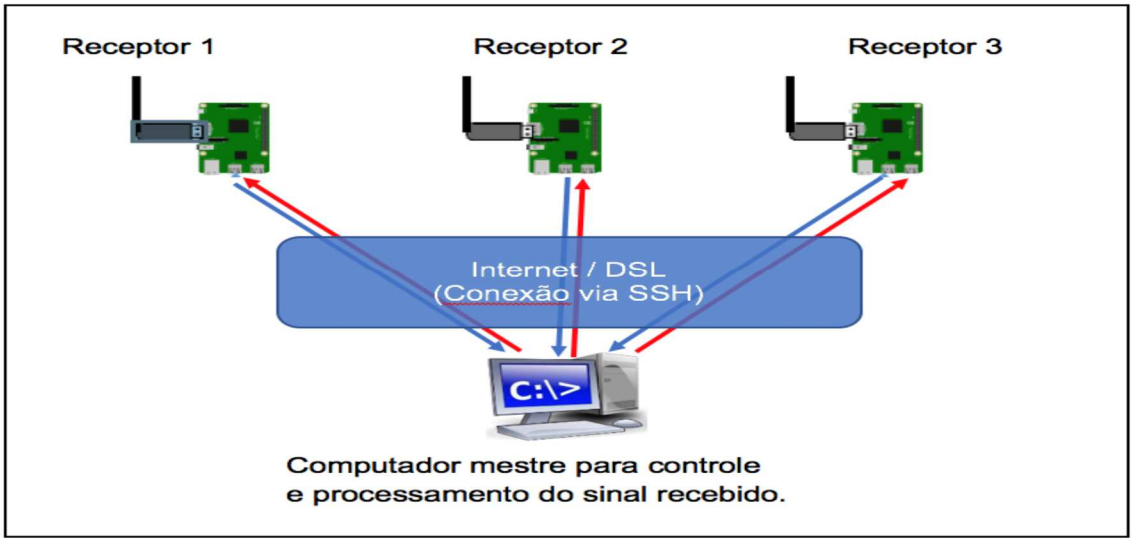


Fonte: Scholl (2017).

Nesse caso, pode-se observar que as hipérboles se cruzaram em dois pontos distintos, ocasionando uma ambiguidade quanto à real posição do emissor. Mesmo obtendo um resultado dúbio, o resultado obtido possui uma precisão relativamente boa, tendo em vista a escala de 1:200m verificada no mapa.

Outro teste realizado teve como alvo um sinal de transmissão FM na frequência 96,9 MHz. Nesse caso, o resultado obtido não foi capaz de fornecer a localização precisa do emissor, tendo em vista estar localizado fora da área compreendida entre os 3 receptores [ver figura 4.5]. Entretanto, apesar do sistema não ter indicado um ponto exato da localização, Scholl verificou que pôde-se obter a direção do sinal (*Direction Finding*) com o resultado, concluindo que o alvo estaria localizado em algum lugar naquela direção.

Figura 8 - Resultado para antena de transmissão FM



Fonte: Scholl (2017).

6 CONCLUSÃO

Após analisar os testes realizados por Scholl (2017) e, considerando a real viabilidade de sua aplicação na localização de sinais, verificou-se a possibilidade da utilização de sistemas e equipamentos, livres de qualquer licença ou assinatura, de baixo custo e grande eficiência, em missões de Guerra Eletrônica.

Destaca-se o fato de o teste ter sido realizado por apenas uma pessoa. Nesse aspecto, vê-se uma considerável vantagem em utilizar esse sistema, visto que, empregando o mesmo esforço de pessoal (ou até mesmo menor), é possível ampliar a área monitorada, sem perder informações ou eficiência.

Somado a isso, levando em consideração que os equipamentos foram instalados em ambientes internos, sem a necessidade de dispô-los em terraços ou torres de antenas, o uso do RTL-SDR se mostrou grande facilitador em operações dos diversos tipos. Tendo como exemplo um ambiente hostil, o fato de instalar um sistema em local aberto, como o terraço de um prédio ou até mesmo um campo aberto, poderia ser um fator preocupante para a equipe de GE em relação à segurança do equipamento e do pessoal envolvido.

Diante do exposto, pode-se concluir que os estudos sobre a GE não devem ser deixados em segundo plano. Pelo contrário, a necessidade de aprimorar o conhecimento sobre o assunto faz-se vital para que se mantenha o acompanhamento das evoluções tecnológicas e, assim, a constante atualização dos sistemas e doutrinas empregados. Nas palavras de Adamy (2001): A chave para entender os princípios da GE (particularmente a parte de radiofrequência) é ter uma compreensão realmente boa da teoria da propagação de rádio. Se você entender como os sinais de rádio se propagam, há uma progressão lógica para entender como eles são interceptados, bloqueados ou protegidos. Sem esse entendimento, parece que é quase impossível abraçar a Guerra Eletrônica. (ADAMY, 2001, p. 5).

Por fim, considerando a eficácia dos testes realizados por Scholl, após demonstrados os resultados obtidos, pôde-se concluir pela eficiência do sistema e entender que, ainda que de forma lenta e gradativa, sua utilização pelas Forças Armadas é viável e pode ser considerada como meio, mesmo que não substitutivo, mas ao menos complementar nas atividades de GE.

REFERÊNCIAS BIBLIOGRÁFICAS

ABU-RGHEFF, Mosa Ali. **Introduction to CDMA Wireless Communications.** Reino Unido. Ed. Elsevier, 2007. Disponível em: <https://books.google.com.br/books?id=SI6Xl8trarEC&printsec=frontcover&dq=inauthor:%22Mosa+Ali+Abu-Rgheff%22&hl=pt-BR&sa=X&ved=0ahUKEwjmu9Ll1ufbAhUDIZAKHcbxB4wQ6AEIKDAA#v=onepage&q&f=false>. Acesso em 18 jun 2018.

ADAMY, David. **EW101**: a first course in electronic warfare. Norwood, MA: Artech House, 2001.

EXÉRCITO BRASILEIRO. **Manual de Campanha:** A GUERRA ELETRÔNICA NA FORÇA TERRESTRE. 2019.

MARTINS, Ramon Mayor. Rádio definido por software – SDR**. IFSC – Santa Catarina,** 2015. Disponível em: <https://wiki.sj.ifsc.edu.br/wiki/images/a/a7/Grupo_de_Estudos_em_R%C3%A1dio_Definido_por_Software.pdf> Acesso em: 2 jun 2018.

OLIVEIRA, Humberto José Corrêa de. **Coletânea história da guerra eletrônica.** V. 1. Brasília, DF: Ministério da Defesa – Centro Integrado da Guerra Eletrônica, 2002.

RTL-SDR.COM. **ABOUT RTL-SDR.** Disponível em: <https://www.rtl-sdr.com/about-rtl-sdr/>. Acesso em: 2 jun 2018.

SCHOLL, Stefan. Introduction and Experiments on Transmitter Localization with TDOA. **Software Defined Radio Academy**, Friedrichshafen, Alemanha. Disponível em: < http://www.panoradio-sdr.de/wp-content/uploads/2017/07/sdr_tdoa_localization_online.pdf>. Acesso em 10 maio 2018.

SRUTHI, M. B. et al. Low cost digital transceiver design for software defined radio using RTL-SDR. **IEE Communications Magazine**, [S. l.], 2013. Disponível em: <https://ieeexplore.ieee.org/abstract/document/6526525>. Acesso em: 8 jun 2018.

STEWART et al. **Software Defined Radio Using MATLAB & Simulink and the RTL-SDR**, Glasgow, Scotland, UK. 2017.

STEWART, Robert W. et al. A Low-Cost Desktop Software Defined Radio Design Environment Using MATLAB, Simulink, and the RTL-SDR. **IEEE Communications Magazine,** [S. l.], 2015.

WIRELESS Innovation Forum. **Introduction to SDR,** [S.l.], [S.d.]. Disponível em <http://www.wirelessinnovation.org/Introduction_to_SDR>. Acesso em: 2 jun 2018.

*Artigo realizado a partir do trabalho de conclusão do Curso Básico de Guerra Eletrônica para Oficiais do Centro de Instrução de Guerra Eletrônica (CIGE) em 2018 pelo Capitão-Tenente Pedro Tebaldi Medeiros da Silva da Marinha do Brasil. Email: tebaldi@marinha.mil.br.

O Processo de Elaboração da Lista de Alvos Cibernéticos no Nível Tático

Ten Cel Com Vinícius Lacerda Vasquez*

RESUMO

A Guerra Cibernética envolve ações que contribuem para a consecução dos objetivos militares, sendo necessária sua integração no planejamento operacional. Neste sentido, este artigo tem o objetivo de apresentar uma proposta para o processo de elaboração da Lista de Alvos Cibernéticos durante o Exame de Situação do comandante tático. Para tanto, desenvolveu-se uma pesquisa qualitativa, de cunho descritivo, e empregou-se, além do método indutivo, um estudo bibliográfico e documental. A pesquisa foi, ainda, orientada no sentido de se compreender as adaptações necessárias ao processo de planejamento de fogos adotado pela doutrina militar terrestre brasileira em função das peculiaridades do ambiente operacional cibernético. A seleção das fontes de pesquisa fundamentou-se em artigos de autores de reconhecida importância no meio literário e acadêmico, bem como em publicações de elevado número de citações ou, ainda, em fontes abertas atuais e disponibilizadas em sítios eletrônicos. Desta forma, a metodologia de elaboração da Lista de Alvos Cibernéticos apresentada permite superar as peculiaridades do espaço cibernético, por meio do emprego de ferramentas auxiliares. Inicialmente, o espaço cibernético é avaliado sobre o prisma da dimensão informacional, a fim de facilitar a compreensão do ambiente operacional e a identificação dos alvos cibernéticos no Teatro de Operações. Em seguida, os alvos adquiridos são analisados empregando-se a taxonomia MACE. Por fim, os alvos identificados nas fases anteriores são selecionados e priorizados utilizando-se o método CRAVER, produzindo-se a Lista de Alvos Cibernéticos. Como conclusão, o artigo destaca a importância do método proposto, bem como apresenta sugestões para trabalhos futuros.

Palavras-chave: Busca de Alvos. Guerra Cibernética. Matriz CRAVER. Taxonomia MACE.

Cyber-Target Listing Process on Tactical Level

ABSTRACT

The Cyber War involves actions that contribute to the achievement of military objectives, being necessary its integration in operational planning. Thus, this article aims to present a proposal for the Cyber-Target Listing methodology during the Military Decision Making Process. Therefore, qualitative research with a descriptive character was developed and, bibliographical and documentary research was employed, besides the inductive method. The research was also oriented to understand the necessary adaptations to the targeting process adopted by the Brazilian military doctrine due to the peculiarities of the cyber operating environment. The selection of research sources was based on articles by authors of recognized importance in the literary and academic circles, as well as publications with a high number of citations or on current open sources available on electronic websites. Thus, the Cyber-Target Listing methodology presented allows overcoming the peculiarities of the cyberspace, through the use of auxiliary tools. Initially, cyberspace is evaluated from the perspective of the informational dimension, to facilitate the understanding of the operating environment and the identification of cyber targets in the theater of operations. The acquired targets are then analyzed using the MACE taxonomy. Finally, the targets identified in the previous phases are selected and prioritized using the CARVER method, producing the Cyber-Target List. In conclusion, the article presents the validity of the proposed method, as well as suggestions for future work.

Keywords: *CARVER Matrix. Cyber Warfare. MACE Taxonomy. Targeting.*

Artigo recebido em 01/12/2019 e aceito para publicação em 1/01/2020

1 INTRODUÇÃO

A Guerra Cibernética tem se mostrado uma opção importante no rol de ações não cinéticas das operações militares. Isto foi motivado pela velocidade da revolução tecnológica recente que culminou na elevação do espaço cibernético à condição de domínio operacional. (US ARMY, 2010; USA, 2018).

Sua transversalidade aos demais domínios (marítimo, terrestre, aéreo e espacial), permite-lhe criar efeitos militares decisivos, produzindo vantagens e influenciando eventos em todos os ambientes operacionais. Entretanto, em um contexto de Operações no Amplo Espectro e à medida que surgem um número maior de atores no ambiente operacional, bem como aspectos relacionados às dimensões humana e informacional, verificase que a complexidade dos problemas enfrentados pelas forças militares aumenta. Para mitigar as consequências deste novo domínio na Defesa Nacional e contrapor os novos desafios apresentados às Forças Armadas na condução das operações militares contemporâneas, em 2008, o Ministério da Defesa incumbiu o Exército Brasileiro das tarefas de coordenar e de integrar as ações de Defesa Cibernética no país. (BRASIL, 2014; EXÉRCITO BRASILEIRO, 2014).

Contudo, com as peculiaridades do domínio cibernético e o fato do conceito de Guerra Cibernética ser uma concepção recente, a doutrina de emprego de suas ações ofensivas ainda carecem de amadurecimento. Neste contexto, este trabalho pretende estudar a aplicação de um método específico para a elaboração da Proposta de Lista de Alvos Cibernéticos (PLA Ciber), durante o Exame de Situação do comandante tático do elemento de Guerra Cibernética.

Para tanto, este artigo está organizado da seguinte maneira: esta primeira seção introdutória, seguida da segunda seção que descreve as peculiaridades do espaço cibernético, da Guerra Cibernética e suas possibilidades. Prossegue pela terceira seção, que introduz ferramentas que subsidiam as etapas do processo de busca de alvos cibernéticos. Quanto a tais etapas, a primeira delas objetiva avaliar o espaço cibernético sobre o prisma das camadas interdependentes física, lógica e cognitiva, facilitando a compreensão do ambiente. A segunda consiste no emprego da taxonomia MACE para a análise dos alvos adquiridos. A última etapa traduz-se na utilização do método CRAVER para a priorização e seleção dos alvos identificados nas fases anteriores. Encerrando o artigo, a quarta seção apresenta as conclusões do estudo, bem como apresenta propostas para trabalhos futuros.

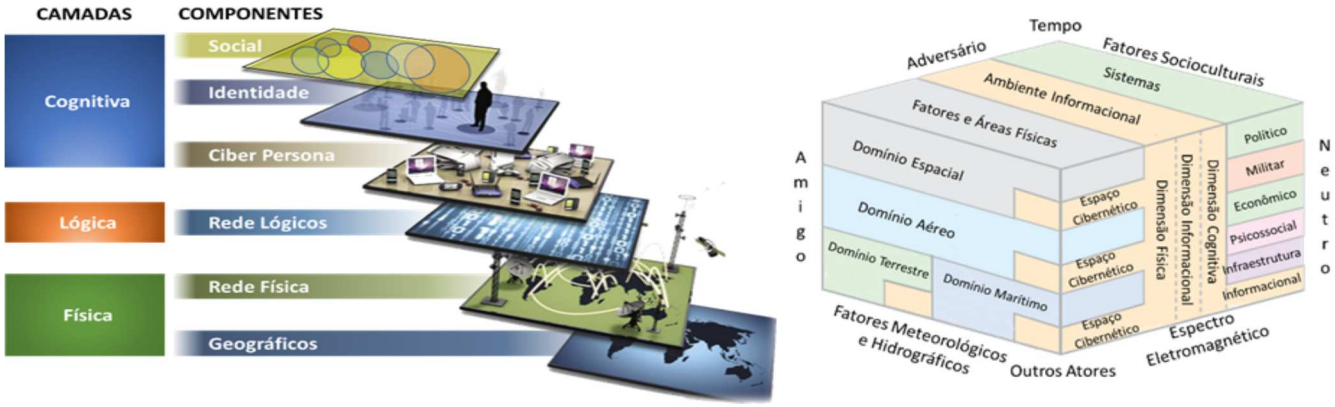
2 O ESPAÇO CIBERNÉTICO E A GUERRA CIBERNÉTICA

O espaço cibernético é um ambiente complexo que vai além dos limites organizacionais e das fronteiras nacionais (BRANDÃO; IZYCKI, 2019). Ele é resultante da interação de pessoas, softwares e serviços disponíveis na Internet por meio de dispositivos e redes de telecomunicações conectados a ela. (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2012).

Na doutrina militar brasileira, o espaço cibernético é caracterizado por ser um ambiente virtual composto por dispositivos computacionais, conectados em redes ou não, onde as informações digitais transitam e são processadas ou armazenadas. Tais atributos criam um espaço operativo comum, integrando as dimensões física, informacional e humana no que se refere a sua dependência aos meios de tecnologia da informação e comunicações. (BRASIL, 2014; EXÉRCITO BRASILEIRO, 2017a; USA, 2018).

A complexidade desse ambiente pode ser minimizada por sua descrição segundo as três perspectivas da dimensão informacional, na qual o espaço cibernético está inserido. A figura 1 representa a inter-relação dessas camadas:

Figura 1— Camadas do Espaço Cibernético e sua visão holística



Fonte: US Army (2010); United Kingdom (2016), adaptador pelo autor. .

A camada física é caracterizada pelo hardware e pela infraestrutura computacional responsáveis pelo armazenamento, transporte e processamento de informações, distribuídos em um espaço geográfico. Seus componentes exigem medidas de segurança física, que podem ser aproveitados para a obtenção do acesso lógico. Ela também define a localização geográfica e a estrutura legal apropriada a ser aplicada nas operações militares, considerando que existem questões de propriedade e soberania ligadas aos domínios físicos e as fronteiras geopolíticas são facilmente ultrapassadas no ciberespaço.(UNITED KINGDOM, 2016; USA, 2018).

A segunda camada refere-se à rede lógica. Essa é uma abstração da camada física e consiste no código de programação, nos protocolos e nos dados que acionam os componentes de rede. Ela restringe o engajamento de seus alvos por meios inerentes ao espaço cibernético, ou seja, um dispositivo ou aplicação projetada para criar um efeito no ciberespaço ou através dele. (UNITED KINGDOM, 2016; USA, 2018).

A última camada é a cognitiva. Ela é responsável por conectar as pessoas ou grupos à sua forma de apresentação no espaço cibernético (ciber-persona). Ela reflete seus aspectos humanos e sociais, incluindo as contas de usuários (humanas ou automatizadas) e de grupos, bem como seus dados e relacionamentos. (UNITED KINGDOM, 2016; USA, 2018).

Essa gama de entidades que interagem nesse domínio para trocarem informações, faz com que ele seja determinante no planejamento operacional (US ARMY, 2019). Deste modo, é fundamental compreender as condições, circunstâncias e fatores que influenciam o ambiente operacional cibernético pois, por meio dele, é possível criar efeitos únicos e decisivos em todos os demais domínios (BRASIL, 2014; USA, 2018).

2.1 PRINCÍPIOS E CARACTERÍSTICAS DA GUERRA CIBERNÉTICA

Para alcançar tais objetivos, o vetor militar a ser utilizado é a Guerra Cibernética. Ela é definida pelas ações no espaço cibernético que amplificam as ações cinéticas e garantem liberdade de ação da força empregada, potencializando seus efeitos no Teatro de Operações. (BRASIL, 2012; EXÉRCITO BRASILEIRO, 2017a).

O termo Guerra Cibernética refere-se, ainda, ao planejamento e à execução das atividades cibernéticas nos níveis operacional e tático de uma operação militar. Ela corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de comando e controle (C2) do adversário. (BRASIL, 2014).

O seu emprego é pautado em quatro princípios relevantes: o efeito, a dissimulação, a rastreabilidade e a adaptabilidade. Os dois primeiros dizem respeito diretamente às ações ofensivas, enquanto os últimos às defensivas. O princípio do efeito remete à produção de impactos no espaço cibernético. Esses devem produzir vantagem em todos os níveis de decisão, afetando o mundo real, mesmo que não sejam cinéticos. A dissimulação trata das medidas a serem adotadas a fim de mascarar a autoria e o ponto de origem das ações ofensivas. A rastreabilidade, por sua vez, está relacionada à detecção das ações cibernéticas do oponente. E, por fim, o princípio da adaptabilidade consiste na capacidade da Guerra Cibernética em adaptar-se e manter a proatividade mesmo diante de mudanças súbitas e imprevisíveis no combate. (BRASIL, 2014).

Uma das principais características da Guerra Cibernética é a insegurança latente dos sistemas computacionais, que parte da premissa de que não há sistemas completamente seguros e que suas vulnerabilidades poderão ser exploradas. Assim, a Guerra Cibernética aproveita-se da ausência das amarras das limitações físicas de distância e espaço e ignora as fronteiras geográficas para conduzir suas ações em qualquer parte do globo. (EXÉRCITO BRASILEIRO, 2017a).

Também há de se observar que o desenvolvimento de armas cibernéticas possui um ciclo mais curto se comparado às tradicionais. Desta maneira, seu custo é inferior aos armamentos cinéticos convencionais. Isto proporciona um desbalanceamento de forças, em que Estados, organizações ou agentes com recursos financeiros limitados são capazes de perpetrar danos tão severos quanto os cometidos por entidades com maiores condições econômicas. (BRANDÃO; IZYCKI, 2019; EXÉRCITO BRASILEIRO, 2017a).

Outro aspecto interessante a ser constatado é a dualidade das ferramentas que podem ser usadas por atacantes e administradores de sistemas com finalidades distintas. Um software de identificação de vulnerabilidades tanto pode ser empregado para identificar falhas em um sistema para a adoção de medidas de proteção, quanto para apresentar oportunidades de ataque. (EXÉRCITO BRASILEIRO, 2017a).

Por este cenário, nota-se que uma operação cibernética pode empregar vários tipos de ataques, disseminados por diferentes vetores,

que exijam níveis de acesso distintos, tudo de forma combinada, sequencial ou simultânea, inclusive conjugar recursos cibernéticos e físicos (BERNIER, 2013). Desta forma, pode-se dizer que o sucesso das ações ofensivas cibernéticas depende do domínio de todo o ciclo de vida do ataque: reconhecimento, preparação, entrega do artefato, exploração, instalação,comando e controle e ações nos objetivos. (BRANDÃO; IZYCKI, 2019; HUTCHINS; CLOPPERT; AMIN, 2011).

Entretanto, é importante destacar que a Guerra Cibernética não tem um fim em si mesma. Ela é tipicamente empregada no contexto de uma Operação Militar, apoiando a condução de outros tipos de operação e contribuindo para a obtenção de um efeito desejado. Todavia, suas ações podem não gerar os resultados esperados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados. Devido a esta incerteza, cada operação deve ser planejada e acompanhada minuciosamente, considerando as particularidades do ciberespaço. (EXÉRCITO BRASILEIRO, 2017a).

2.2 GUERRA CIBERNÉTICA COMO MEIO NÃO CINÉTICO DE APOIO AO COMBATE

Para fins de aplicação do poder de combate, estão definidas três capacidades operativas: proteção, exploração e ataque. A atividade de proteção cibernética é de caráter permanente e refere-se à condução de tarefas para neutralizar as ações ofensivas do oponente sobre os ativos computacionais, redes de computadores e de comunicações. A de exploração tem o objetivo de preparar os alvos cibernéticos para ações futuras. Isso se dá por meio do mapeamento dos sistemas e dos ativos de informação presentes no espaço cibernético de interesse, bem como da identificação e exploração de suas vulnerabilidades. Por sua vez o ataque é caracterizado pela interrupção, negação, degradação, corrupção ou destruição de informações, de sistemas, de dispositivos ou de redes computacionais ou de comunicações do oponente. (EXÉRCITO BRASILEIRO, 2017a).

Das três capacidades operativas descritas acima, as ações de exploração e de ataque cibernético configuram a atuação não cinética da Guerra Cibernética. Seu emprego provoca efeitos no ambiente físico, podendo ser executados simultaneamente às ações cinéticas para causar resultados complementares sobre um mesmo alvo, sem o emprego do fogo cinético. (BRANDÃO; IZYCKI, 2019; EXÉRCITO BRASILEIRO, 2015, 2017a).

Em geral, estas ações afetam as propriedades básicas da segurança da informação: confidencialidade, integridade e disponibilidade. Desta forma, é imprescindível que a análise e o planejamento de Guerra Cibernética sejam orientados por estes elementos, permitindo seu emprego de maneira seletiva e pontual, engajando objetivos elencados pelos diversos níveis (estratégico, operacional e tático). Destaca-se, ainda, a possibilidade de se considerar outros atributos complementares, tais como: autenticidade, confiabilidade, conformidade, legalidade, não repúdio (irretratabilidade) e responsabilidade. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013; EXÉRCITO BRASILEIRO, 2017a, 2017b).

Com a capacidade de causar danos ou baixas nas estruturas físicas, nos centros de C2, nas redes de computadores, nos centros de comunicações, afetar o moral das tropas adversárias ou, ainda, reduzir a possibilidade do inimigo de explorar o ambiente operativo, é pelas ações de exploração e de ataque que a Guerra Cibernética se integra à função de combate Fogos (EXÉRCITO BRASILEIRO, 2015), cuja definição é:

> [...] um conjunto de atividades, tarefas e sistemas integrados, [que] permitem a aplicação e o controle de fogos, orgânicos ou não, integrados pelos processos de planejamento e coordenação. [...] Para isso, os sistemas de fogos devem estar integrados, considerando os meios conjuntos e incorporando a defesa antiaérea e a capacidade de realizar ações eletrônicas e cibernéticas. (EXÉRCITO BRASILEIRO, 2015, p. 1-1).

A responsabilidade da integração dos fogos com os atuadores não cinéticos é da célula de Coordenação de Fogos. Para tanto, ela conta com uma equipe multidisciplinar e especializada incumbida de avaliar todas as possibilidades e limitações dos meios disponíveis, buscando a eficácia do apoio de fogo. A tarefa de sincronização desses meios de intervenção no combate é encargo do Grupo Integrado de Seleção e Priorização de Alvos (GISPA). Dentre os elementos que podem integrar esse grupo, o Oficial de Ligação de Guerra Cibernética é responsável pelo assessoramento quanto às possibilidades dos atuadores dessa capacidade. (EXÉRCITO BRASILEIRO, 2017b).

Em relação aos elementos de Guerra Cibernética com capacidade ofensiva no nível tático, quando for ativada a Estrutura Militar de Defesa, esses poderão englobar uma Força Conjunta de Guerra Cibernética, como Força Componente, para executar as operações cibernéticas em proveito do Teatro de Operações ou da Área de Operações (TO/AO), bem como estruturas de Guerra Cibernética de cada uma das demais

Forças Componentes. Na Força Terrestre Componente (FTC), o planejamento e o assessoramento atinentes às ações cibernéticas ofensivas é encargo do comandante do Batalhão de Guerra Eletrônica, enquanto o comandante do Batalhão de Inteligência Militar é responsável pelas ações de Inteligência Cibernética. (BRASIL, 2011; EXÉRCITO BRASILEIRO, 2017a).

3 O PROCESSO DE BUSCA DE ALVOS CIBERNÉTICOS

O processo de busca de alvos é uma das tarefas que integram a função de combate Fogos e define a fase inicial do processo de planejamento de fogos. Ele é caracterizado por sua recursividade e continuidade, que perdura desde o tempo de paz e se prolonga ao logo de toda a campanha. Para tanto, engloba os processos de aquisição, de seleção e de análise de alvos. (EXÉRCITO BRASILEIRO, 2017b).

Sua execução vai além de possibilitar o apoio de fogo, favorecendo o emprego de outros vetores, incluindo os não cinéticos, tal como a Guerra Cibernética. Ela baseia-se nas diretrizes de fogos do escalão superior, sendo diretamente influenciada pela oportunidade, pela possibilidade de gerar efeitos colaterais e pela legalidade. No nível tático, ele inicia quando o comandante da força interpreta a missão e começa seu exame de situação (EXÉRCITO BRASILEIRO, 2017b).

Na Guerra Cibernética, sua concretização obedece à sistemática adotada na doutrina militar, sendo parte do planejamento detalhado do comandante do elemento de cibernética do escalão considerado. Entretanto, face às peculiaridades do espaço cibernético, fazem-se necessárias adaptações no seu modelo de planejamento, buscando criar soluções alternativas para contornar a complexidade do ciberespaço e sua rápida adaptação ao desenvolvimento das ações. (EXÉRCITO BRASILEIRO, 2017a).

Seu principal produto é a Proposta de Lista de Alvos Cibernéticos (PLA Ciber) que será consolidada pelos elementos de coordenação de fogos de cada escalão em presença na Lista Integrada Priorizada de Alvos (LIPA). (EXÉRCITO BRASILEIRO, 2017a).

A seguir, serão abordadas as três fases que compreendem o processo de busca de alvos: aquisição de alvos; análise de alvos; e seleção de alvos.

3.1 PRIMEIRA FASE: AQUISIÇÃO DE ALVOS CIBERNÉTICOS

A aquisição de alvos é um processo cíclico e consiste na detecção e localização de um objetivo com o detalhamento suficiente para permitir o efetivo emprego de armas. Ele inicia antes da campanha militar propriamente dita com a elaboração do Levantamento Estratégico de Área (LEA) e das pastas e listas de alvos e perdura durante todas suas fases. Nessas bases de dados, encontram-se os elementos que facultam o estudo detalhado da área e as informações conhecidas sobre os alvos de interesse, necessárias para o emprego das capacidades militares. (EXÉRCITO BRASILEIRO, 2001, 2017b).

Na análise de Guerra Cibernética, ele tem início com o recebimento dos planos e diretrizes do escalão superior. Nessa fase, o comandante e seu Estado-Maior buscarão entender, visualizar e descrever o ambiente operacional, especialmente o espaço cibernético, facilitando a compreensão da missão e a análise do problema. Para tanto, pode-se utilizar as técnicas de planejamento conceitual, bem como a análise dos fatores operacionais e de decisão, o que permite a revalidação contínua do planejamento. (EXÉRCITO BRASILEIRO, 2014).

Durante a definição do ambiente operacional cibernético, é natural considerar os meios de comunicações e de TI, bem como a informação em si. Entretanto, outras variáveis que também interagem com a informação e os ativos computacionais e de comunicação também devem ser ponderados, tais como indivíduos e organizações. (US ARMY, 2019).

Em sequência, devem ser identificados outros alvos potenciais existentes no interior da área de operações e de interesse da FTC, passíveis de exploração e de ataque cibernético. Nesta fase, a Inteligência terá papel fundamental no detalhamento dos componentes do alvo ou dos sistemas de alvos e suas vulnerabilidades. Como insumo, é utilizada a base de dados de alvos elaborada desde o tempo de paz. (EXÉRCITO BRASILEIRO, 2017b).

Nesta etapa, também são elencadas as Necessidades de Inteligência que comporão o Plano de Obtenção do Conhecimento. Para tanto, faz-se necessário considerar cada uma das camadas do espaço cibernético no seu estabelecimento, conforme apresentado de forma resumida no Quadro 1. Destaca-se, ainda, que o comandante do elemento de cibernética tático deve contar com meios variados de obtenção, além da fonte cibernética, para conseguir ou confirmar informações sobre os alvos a serem batidos. (EXÉRCITO BRASILEIRO, 2017b).

Quadro 1 – Necessidades de Inteligência no Espaço Cibernético

Camada	Necessidades de Inteligência
Cognitiva	- Uso do espaço cibernético pelo oponente. - Elementos ou entidades, da força oponente ou não, interessados ou com a capacidade de acessar dados e informações de interesse. - Consumidores de dados e informações nas áreas de operações e de influência. - *Hackers* e entidades presentes nas áreas de operações e de influência que podem ser cooptados. - Relação dos atores locais com as camadas da rede física (telefonia celular, cibercafé, *LAN-Houses*) e da rede lógica (*sites* e aplicações). - Influenciadores digitais capazes de interferir no ambiente operacional.
Lógica	- Páginas *web* que induzem ou tenham impacto social nas áreas de operações e de influência. - Configurações de rede, softwares e sistemas criptográficos utilizados pelo oponente e suas possíveis vulnerabilidades. - Endereços e protocolos pelos quais os dados de interesse podem ser acessados na Internet. - Softwares utilizados na àrea de Operações. - Métodos de intrusão e como eles podem ser mascarados.
Física	- Sistemas de C2 do oponente presentes nas áreas de operações e de influência. - Pontos críticos de comunicações, presentes nas áreas de operações e de influência, que o oponente possa utilizar em seu proveito ou que possam servir de meio de entrada nas suas redes. - Localização dos ativos de rede existente nas áreas de operações e de influência, tais como cabos de fibra ótica, pontos de troca de tráfego da Internet, locais públicos com pontos de acesso à Internet (cyber cafés e *LAN-Houses*), centros de processamento de dados e *intranets* militares ou governamentais. - Medidas de segurança física implementadas que possam impedir o acesso a esses ativos.

Fonte: US Army (2019), adaptado pelo autor.

Na camada Cognitiva, destaca-se que um indivíduo pode possuir várias ciber-personas que o representam de maneiras diferentes no ciberespaço, inclusive sem refletir suas características físicas reais. Por outro lado, uma única identidade cibernética pode ter vários usuários. Isto dificulta a atribuição de responsabilidades e demanda o apoio significativo da atividade de Inteligência para gerar a correta compreensão do ambiente operacional a fim de orientar o emprego da força ou criar o efeito desejado. (UNITED KINGDOM, 2016).

3.2 SEGUNDA FASE: ANÁLISE DE ALVOS CIBERNÉTICOS

Com a definição dos alvos potenciais a serem engajados, realiza-se a análise de suas caraterísticas e de seu relacionamento com os aspectos operativos da campanha militar. O estudo desses fatores auxilia na determinação de sua importância militar, a oportunidade para o ataque e a seleção do método de ataque mais conveniente para engajá-lo. (EXÉRCITO BRASILEIRO, 2017b).

A importância militar de um alvo é atribuída de acordo com a ameaça que este representa para o cumprimento da missão da força. Ela poderá vir especificada nas diretrizes no escalão superior ou deverá ser determinada durante os trabalhos de Estado-Maior, a quem compete apreciar a maneira que contribuem para atingir o Efeito Final Desejado ou colaboram para a conquista de Pontos Decisivos ou dos objetivos elencados pelo escalão enquadrante. Assim, será possível classificá-los de acordo coma sua natureza: estratégico, operacional ou tático. (EXÉRCITO BRASILEIRO, 2014, 2017b).

Para os passos seguintes, a taxonomia MACE (acrônimo de *Military Activities and Cyber Effects*) mostra-se uma ferramenta auxiliar valiosa. Ela consiste em um modelo criado pelo Centro de Pesquisa e Desenvolvimento de Defesa do Canadá para Pesquisa e Análise Operacional (DRDC CORA)para investigar o impacto dos efeitos cibernéticos nas decisões de comando e como integrar os recursos cibernéticos ao processo de planejamento operacional. Para isso, ela associa o tipo de ataque cibernético ao vetor de ataque e ao nível de acesso necessário para iniciá-lo, correlacionando-a com os tipos de adversário e os efeitos a serem produzidos. (BERNIER, 2013).

O Quadro 2 descreve as categorias, de interesse para este trabalho, que compõem a Taxonomia MACE:

Quadro 2 – Descrição das seis categorias da taxonomia MACE

Categoria	Descrição
Ações Táticas	Ações táticas que produzem efeitos militares sobre o espaço cibernético.
Efeitos Cibernéticos	Descrição dos efeitos que podem ser produzidos no ambiente cibernético empregando os vários tipos de ataques cibernéticos. Compreendem a interceptação, modificação, degradação, fabricação e interrupção.
Tipos de Ataques	Abrange os tipos mais significativos de ataques cibernéticos, sejam eles passivos ou ativos.
Nível de Acesso	Descreve os diferentes níveis de acesso ao sistema ou rede, determinando as restrições impostas ao operador cibernético e os privilégios de acesso exigidos para cada tipo de ataque. São quatro: sem a necessidade de privilégios, necessidade de privilégios limitada, privilégio administrativo e acesso físico.
Vetores de Ataque	Relação dos métodos e das ferramentas usadas para se infiltrar em computadores e instalar o artefato malicioso. Dividem-se em mecanismos e ferramentas.

Fonte: Bernier (2013), adaptado pelo autor.

A oportunidade para engajar um alvo cibernético está relacionada com suas características e limitações. Para tanto, o planejador deve, inicialmente, relacionar a ação tática a ser realizada com o efeito a ser provocado na dimensão informacional. (BERNIER, 2013; EXÉRCITO BRASILEIRO, 2017a, 2017b; US ARMY, 2019).

Por fim, a seleção do método de ataque procura a técnica operacional cibernética a ser empregada para se provocar o efeito desejado com o nível de acesso mínimo requerido, os vetores de ataque disponíveis, entre outros elementos que definem o alvo como compensador ou não. (BERNIER, 2013).

Como produto desta etapa, tem-se uma lista preliminar de alvos a serem engajados, que serão priorizados na fase seguinte. (EXÉRCITO BRASILEIRO, 2017b).

3.3 TERCEIRA FASE: SELEÇÃO DE ALVOS CIBERNÉTICOS

Nesta última fase, os meios do oponente identificados e analisados anteriormente serão relacionados nas listas de alvos disponíveis e priorizados de acordo com a avaliação de suas vulnerabilidades e da situação tática. Para tanto, propõe-se a utilização do método de priorização de alvos conhecido pelo acrônimo CRAVER (criticabilidade, recuperabilidade, acessibilidade, vulnerabilidade, efeitos e reconhecibilidade). (EXÉRCITO BRASILEIRO, 2017a, 2017b).

O quadro 3 apresenta as descrições de cada uma das seis categorias:

Quadro 3 – Categorias do método de avaliação CRAVER

Categoria	Descrição
Criticabilidade	Refere-se à importância ou ao valor do alvo no contexto da campanha militar. É medido segundo o grau de comprometimento ou dos elementos críticos do ativo analisado. Ela depende de diversos fatores, tais como tempo para alcançar o efeito desejado, existência de sistemas legados e impacto sobre a funcionalidade do alvo. No campo da segurança da informação, a criticabilidade ainda corresponde à da confidencialidade, integridade ou disponibilidade do ativo informacional.
Recuperabilidade	É a capacidade de ser restabelecer a funcionalidade, total ou parcial, do alvo. É medido com base no tempo estimado para a recuperação do dano infligido ao ativo, considerando inclusive, a existência de *backup* do sistema ou dos dados. A recuperabilidade é inversamente proporcional ao valor do alvo, ou seja, quanto maior a recuperabilidade de um alvo, menor a sua relevância para as operações.
Acessibilidade	Compreende a avaliação das condições que influenciam o acesso ao alvo para a realização do ataque. Está associada às medidas de segurança físicas e lógicas adotadas pelo oponente. Pode considerar, ainda, o grau de adestramento do pessoal de TI, da educação cibernética da tropa e a necessidade de acesso físico ao ativo.
Vulnerabilidade	Refere-se ao grau de conhecimento necessário e os meios disponíveis para a exploração do alvo, bem como sua suscetibilidade às diferentes formas de ataque. Deve considerar, ainda, a necessidade do desenvolvimento dos artefatos para a exploração ou do conhecimento de uma ou mais vulnerabilidades *Zero-Day*.
Efeitos	O alvo deve ser atacado apenas se os efeitos desejados estiverem coerentes com os objetivos que se deseja atingir. Ainda deve-se considerar as consequências, diretas ou indiretas, provocadas pelo ataque sobre as demais operações e a população local, levando em conta os riscos de efeitos colaterais, as restrições impostas pelo Direito Internacional Humanitário (DIH) e pelo Direito Internacional dos Conflitos Armados (DICA).
Reconhecibilidade	Traduz a capacidade de identificar um ativo como alvo. É avaliado o quão fácil é buscar e coletar informações sobre o alvo sem ativar as contramedidas de segurança. Deve considerar, ainda, a necessidade do acesso físico ao ativo.

Fonte: Exército Brasileiro (2017b) e Schnaubelt, Larson, Boyer (2014), adaptado pelo autor.

Sua aplicação consiste na atribuição de pesos para cada um dos seis critérios, a fim de determinar o impacto sobre cada alvo, construindo-se uma matriz. A faixa de pontuação dos critérios é subjetiva, podendo ter seus limites inferior e superior definidos de acordo com a percepção do planejador. Após a valoração dos seis critérios em cada alvo, suas pontuações são somadas, determinando a prioridade do alvo. A pontuação final dos alvos também é relativa e a matriz pode ser reavaliada de acordo com a missão e os requisitos operacionais, bem como a percepção e experiência do planejador. (SCHNAUBELT; LARSON; BOYER, 2014).

3.4 PROPOSTA DE LISTA DE ALVOS CIBERNÉTICOS

Ao término do processo de busca de alvos cibernéticos, o Estado-Maior terá produzido a Proposta de Alvos Cibernéticos que substanciará a construção das Linhas de Ação do comandante tático de cibernética. Esta lista também será integrada ao planejamento dos demais meios de apoio de fogo pelos elementos de coordenação de fogos de cada escalão em presença, até a aprovação da Lista Integrada Priorizada de Alvos (LIPA). (EXÉRCITO BRASILEIRO, 2017a).

4 CONCLUSÃO

As ações de Guerra Cibernética geram efeitos nos domínios físicos e produzem a liberdade de ação necessária para a condução das operações militares. Assim, elas contribuem decisivamente para se alcançar o Efeito Final Desejado, os Pontos Decisivos ou conquistar objetivos táticos. Para tanto, a elaboração dos planos e ordens envolve uma metodologia particular que combina arte e ciência no intuito de solucionar o problema militar.

Como forma de auxiliar o planejamento detalhado do comandante tático do elemento de cibernética, este artigo abordou uma proposta de método de busca de alvos cibernéticos por meio da correlação da análise do ambiente operacional cibernético com duas ferramentas auxiliares: a

taxonomia MACE e a matriz CRAVER. Isto foi motivado devido à complexidade do domínio cibernético, potencializado por suas peculiaridades, e pelo fato do planejamento de fogos tradicional estar focado no emprego dos meios cinéticos.

Na fase de aquisição de alvos, a fim de proporcionar o entendimento do ambiente operacional cibernético, o ciberespaço foi observado sob o prisma da dimensão informacional, que o divide em três camadas interdependentes (física, lógica e social). Na fase de análise de alvos, foi empregada, a taxonomia MACE, a fim de se investigar o impacto dos efeitos cibernéticos nas decisões de comando e a integração dos recursos cibernéticos ao processo de planejamento operacional. Por fim, na fase de seleção dos alvos cibernéticos, foi empregada a matriz CRAVER na priorização de alvos elencados nas fases anteriores.

Estas três ferramentas associadas mostraram-se um método coerente para ser aplicado na elaboração da Proposta de Lista de Alvos Cibernéticos. Embora estas técnicas não sejam inéditas, a sua aplicação é inovadora no processo de busca de alvos cibernéticos.

Como proposta de trabalhos futuros, sugere-se a validação do modelo apresentado em exercícios e simulações, possibilitando a realização de estudos de caso. Após sua ratificação ou aperfeiçoamento, visualiza-se, ainda, a oportunidade de desenvolver-se um sistema dotado de inteligência artificial, capaz de realizar o processo de busca de alvos em curto espaço de tempo, permitindo a detecção, identificação, análise e distribuição dos dados sobre alvos compensadores de maneira automática. Tudo isto contribuirá para a evolução da doutrina militar no campo da cibernética e de planejamento de fogos.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**: tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro: ABNT, 2013.

BERNIER, M. **Military Activities and Cyber Effects (MACE) Taxonomy**: TM 2013-226. Ottawa: DRDC CORA, 2013.

BRANDÃO, J. E. M. D. S.; IZYCKI, E. A. Poder Ofensivo no Espaço Cibernético. In: ANDRADE, I. D. O., et al. **Desafios contemporâneos para o Exército Brasileiro**. Brasília, DF: Ipea, 2019. cap. 10, p. 241-273. Disponível em: <http://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/180826_desafios_contemporaneos_para_o_exercito_brasileiro.pdf>. Acesso em: 28 ago. 2019.

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas**: MD30-M-01. Brasília, DF: Ministério da Defesa, 2011. v. 1.

BRASIL. Ministério da Defesa. **Política de Defesa Cibernética**: MD31-P-02. Brasília, DF: Ministério da Defesa, 2012.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**: MD31-M-07. Brasília, DF: Ministério da Defesa, 2014.

EXÉRCITO BRASILEIRO. **Estratégia**: C-124. 3. ed. Brasília, DF: Estado-Maior do Exército, 2001.

EXÉRCITO BRASILEIRO. **Processo de Planejamento e Condução das Operações Terrestres**: EB20-MC-10.211. Brasília, DF: Estado-Maior do Exército, 2014.

EXÉRCITO BRASILEIRO. **Fogos**: EB20-MC-10.206. Brasília, DF: Estado-Maior do Exército, 2015.

EXÉRCITO BRASILEIRO. **Guerra Cibernética**: EB70-MC-10.232. Brasília, DF: Comando de Operações Terrestres, 2017a.

EXÉRCITO BRASILEIRO. **Planejamento e Coordenação de Fogos**: EB70-MC-10.346. Brasília, DF: Comando de Operações Terrestres, 2017b.

HUTCHINS, E. M.; CLOPPERT, M. J.; AMIN, R. M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In: INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY, 6., 2011, Washington, DC. **Proceedings** […]. p. 113-125. Disponível em: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>. Acesso em: 23 ago. 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27032:** Information Technology - Security Techniques - Guidelines for Cybersecurity. Geneva: ISO/IEC, 2012.

SCHNAUBELT, C. M.; LARSON, E. V.; BOYER, M. E. **Vulnerability Assessment Method Pocket Guide:** a tool for center of gravity analysis. Santa Monica, CA: RAND Corporation, 2014. 142 p.

UNITED KINGDOM. Ministry of Defence. **Cyber Primer**. 2. ed. Swindon: Development, Concepts and Doctrine Centre of Ministry of Defence, 2016. Disponível em: <www.gov.uk/mod/dcdc>. Acesso em: 5 set. 2019.

US ARMY. **Cyberspace Operations Concept Capability Plan 2016-2028:** TRADOC Pamphlet 525-7-8. Newport News: U.S. Army Capabilities Integration Center, 2010.

US ARMY. **Intelligence Preparation of the Battlefield:** ATP 2-01.3. Washington, DC: Department of the Army, 2019.

USA. Departament of Defense. **Cyberspace Operations:** JP 3-12. Washington: Departament of Defense, 2018.

*Artigo realizado a partir do trabalho de conclusão do Curso de Especialização em Planejamento de Guerra Eletrônica (CIGE) e de Guerra Cibernética em apoio às Operações em 2019 pelo Tenente Coronel de Comunicações Vinícius Lacerda Vasquez do Exército Brasileiro. E-mail: lacerda.vinícius@eb.mil.br.

Atuação colaborativa da Defesa Cibernética na proteção de infraestruturas críticas de interesse para a Defesa Nacional

Ten Cel Com Walbery Nogueira de Lima e Silva*

RESUMO

O horizonte cibernético da próxima década tende a ampliar a conexão global, trazendo mais usuários para este domínio e ofertando novas tecnologias, tais como redes 5G e inteligência artificial. As ameaças poderão empregar o espaço cibernético para ações que geram efeitos cinéticos e não cinéticos sobre infraestruturas críticas (IEC) de interesse para a Defesa Nacional, com o risco de provocar paralisia estratégica no funcionamento de países, conforme já ocorreu nos ataques à Estônia (2007) e à Ucrânia (2014). As Forças Armadas estão diretamente ligadas a este tema, uma vez que dependem de produtos e serviços do setor privado para manterem a operacionalidade e, no caso de grave crise, poderão ter tropas empregadas no contexto da Defesa Nacional. Este artigo levanta a importância da atuação colaborativa envolvendo governo, defesa, academia e setor privado, aliada à cooperação internacional, como forma de incrementar a resiliência cibernética. É apresentada a experiência do Comando de Defesa Cibernética na condução do exercício interagências Guardião Cibernético (EGC). A atividade simulada, ocorrida em julho de 2019, contou com a participação de empresas e organizações dos setores elétrico, financeiro, nuclear e de telecomunicações, bem como de observadores internacionais do Cooperative Cyber Defence Center of Excelence da OTAN e de nações amigas. O EGC permitiu praticar processos de tomada de decisão e procedimentos técnicos. Neste artigo são evidenciados a concepção do exercício, os ensinamentos colhidos para a proteção de IEC e a evolução do EGC que na 3ª edição terá cenário cibernético contendo desafios da próxima década e a inclusão dos setores de transporte aéreo e de fornecimento de água.

Palavras-chave: Espaço cibernético. Atuação colaborativa. Infraestruturas críticas.

Collaborative approach of Cyber Defense to protect critical infrastructure of interest for National Defense

ABSTRACT

The cyber horizon of the next decade tends to broaden the global connection, bringing more users into this domain and expanding new technologies such as 5G networks and artificial intelligence. Threats can use cyberspace for actions that result in kinetic effects and non-kinectic effects on National Defense critical infrastructure (CI) with the risk of causing strategic paralysis in the countries, as occurred in the attacks on Estonia (2007) and Ukraine (2014). The Armed Forces are directly tied to this issue because they rely on private sector products and services to maintain their operationality and in case of an incident with severe crisis troops may be deployed. This essay moots the importance of collaborative approach involving government, defense, academia and the industry, integrated with international cooperation in a unity of effort to enhance cyber resilience. It is presented the interagency exercise Cyber Guardian (CG) study case that is coordinated by the Brazilian Cyber Defense Command. The second edition of this drill, which took place in July 2019, was attended by companies and organizations from the electrical, financial, nuclear and telecommunications sectors as well as international observers from NATO Cooperative Cyber Defense Center of Excellence and partner nations. The CG aims to practice decision-making processes and technical procedures. This article presents the exercise specification, lessons learned to increase critical infrastructure protection and CG evolution that in 3rd edition will have incident scenarios regarding cyber challenges for the next decade as well as the addition of air transport and water supply sectors.

Keywords: *Cyberspace. Collaborative approach. Critical infrastructure.*

Artigo recebido em 01/12/2019 e aceito para publicação em 1/01/2020

1 INTRODUÇÃO

A próxima década sinaliza a adoção de novos recursos que serão disponibilizados para o funcionamento da sociedade moderna cada vez mais dependente de tecnologias que serão usadas para potencializar a capacidade de operação das infraestruturas críticas (IEC) e para elevar a um novo patamar a variedade de serviços ao usuário final no mundo interconectado (NATO, 2019).

Ao mesmo tempo, as ameaças cibernéticas tendem a continuar explorando vulnerabilidades para fins diversos, tais como espionagem, hacktivismo, terrorismo e ações perpetradas por estados nação, o que pode conduzir a cenários catastróficos de paralisia estratégica de países. A história recente revela exemplos disso, conforme ataques cibernéticos de grande impacto nacional ocorridos na Estônia em 2007 e na Ucrânia em 2014 (E-ISAC, 2016).

Ressalta-se que as Forças Armadas (FA) têm uma ligação direta com este tema, uma vez que é cliente de muitos serviços e produtos oriundos da indústria para ter sua plena capacidade operativa, bem como poderá ser acionada para restabelecer a lei e a ordem no caso de ataque cibernético de grande envergadura que comprometa a segurança interna, conforme prevê o Sistema Militar de Defesa Cibernética (Ministério da Defesa, 2014).

Em meio a esse ambiente interconectado, de ações no mundo virtual que podem gerar efeitos cinéticos, a atuação colaborativa envolvendo governo, defesa, academia e setor privado, aliada à cooperação internacional, mostra-se como um caminho desejável para garantir a unidade de esforço necessária ao incremento da resiliência cibernética. Quais ações podem ser feitas nesse sentido? Qual seria o papel das FA em situação de guerra e de não-guerra?

Este artigo levanta a importância da atuação integrada em ambiente interagências, apresentando como estudo de caso o Exercício Guardião Cibernético (EGC), o qual é conduzido anualmente pelo Comando de Defesa Cibernética (ComDCiber) e é voltado para a proteção de infraestruturas críticas (IEC) de interesse para a Defesa Nacional.

A 2ª edição do EGC foi realizada no período de 02 a 04 de julho de 2019, nas instalações do ComDCiber e do Centro de Instrução de Guerra Eletrônica (CIGE), contando com a participação de 215 representantes de 41 empresas e organizações.

O exercício está alinhado com a Política Nacional de Segurança da Informação (PNSI) e com a Estratégia Nacional de Segurança Cibernética (E-Ciber) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), as quais preveem a elevação do nível de proteção do governo e das infraestruturas críticas por meio de ações baseadas na cooperação.

2 DESENVOLVIMENTO

2.1 CONCEPÇÃO DO EGC 2.0

O EGC 2.0 teve por finalidade contribuir para o incremento do nível de proteção do espaço cibernético nas infraestruturas críticas de interesse para a Defesa Nacional nos seguintes setores: elétrico, financeiro, nuclear e telecomunicações.

Para o cumprimento do seu propósito, foram estabelecidos os seguintes objetivos:

a) coordenar e integrar, em ambiente interagências, a segurança e defesa cibernéticas para a proteção de infraestruturas críticas;

b) exercitar o processo decisório em diferentes níveis de responsabilidade e de competência, incentivando a atuação colaborativa na prevenção, solução e mitigação de danos causados por ameaças existentes no espaço cibernético;

c) verificar a efetividade de procedimentos para a solução de incidentes em infraestruturas críticas;

d) contribuir para a integração do governo, defesa, comunidade acadêmica e setor privado, por meio de simulações virtual e construtiva, bem como propondo contribuição de normativas;

e) aplicar boas práticas de proteção cibernética nas ações preventivas e reativas frente a incidentes cibernéticos;

f) empregar ferramentas para o compartilhamento de informação; e

g) proporcionar ambiente favorável para que as empresas e organizações simulem incidentes que permitam colher ensinamentos para o aprimoramento de processos e protocolos internos.

O exercício contou com a participação de representantes de diversas áreas de interesse para o ecossistema cibernético, conforme descrito a seguir:

Quadro 1— Participantes do EGC 2.0

Área Estratégica	Participantes
Defesa	Chefia de Operações Conjuntas (CHOC), Assessoria de Doutrina e Legislação (ADL), Comissão Interescolar de Doutrina de Operações Conjuntas (CIDOC), Diretoria de Comunicações e de Tecnologia da Informação da Marinha (DCTIM), CTIM, CITEx, Comando de Comunicações e de Guerra Eletrônica do Exército (Cmdo Com GE Ex), Departamento de Controle do Espaço Aéreo (DECEA) e Centro de Computação da Aeronáutica em Brasília (CCA BR).
Setor Elétrico	Operador Nacional do Sistema Elétrico (ONS), Agência Nacional de Energia Elétrica, Itaipu Binacional, Companhia de Transmissão de Energia Elétrica Paulista e Furnas.
Setor Financeiro	Banco Central (Bacen), Federação Brasileira de Bancos, Banco do Brasil, Caixa Econômica Federal, Banco Bradesco, Banco Itaú, Banco Santander, B3 Infraestrutura de mercado financeiro, Comissão de Valores Mobiliários e Câmara Interbancária de Pagamentos.
Setor Nuclear	Departamento de Coordenação do Sistema de Proteção ao Programa Nuclear Brasileiro (DCSIPRON-GSI/PR), Comissão Nacional de Energia Nuclear, Indústrias Nucleares Brasileiras, Eletrobras, Eletronuclear, Instituto de Pesquisas Energéticas e Nucleares, Centro Tecnológico da Marinha em São Paulo, Agência Internacional de Energia Atômica e Universidade de São Paulo.
Setor de Telecomunicações	Agência Nacional de Telecomunicações (Anatel), CLARO, OI, Telebras, Telefônica e TIM.
Órgãos Parceiros	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, Centro de Tratamento de Incidentes de Rede do Governo, Agência Brasileira de Inteligência, Divisão de Tecnologias Sensíveis do Ministério das Relações Exteriores, Serviço de Repressão a Crimes Cibernéticos do Departamento da Polícia Federal, Serviço Federal de Processamento de Dados e Rede Nacional de Ensino e Pesquisa.
Comunidade Acadêmica	Escola Superior de Guerra, Universidade de Campinas e Universidade de São Paulo.
Observadores Internacionais	Agência Internacional de Energia Atômica (AIEA), Centro Cooperativo de Excelência em Defesa Cibernética da OTAN (CCDCOE), empresa SAAB de desenvolvimento do projeto FX-2 Gripen, bem como adidos e representantes dos Estados Unidos da América, Portugal, Suécia e Tailândia .

Fonte: o autor, 2019.

2.2 ESTRUTURA DE SIMULAÇÃO

O exercício adotou técnicas de simulação virtual e construtiva de forma integrada.

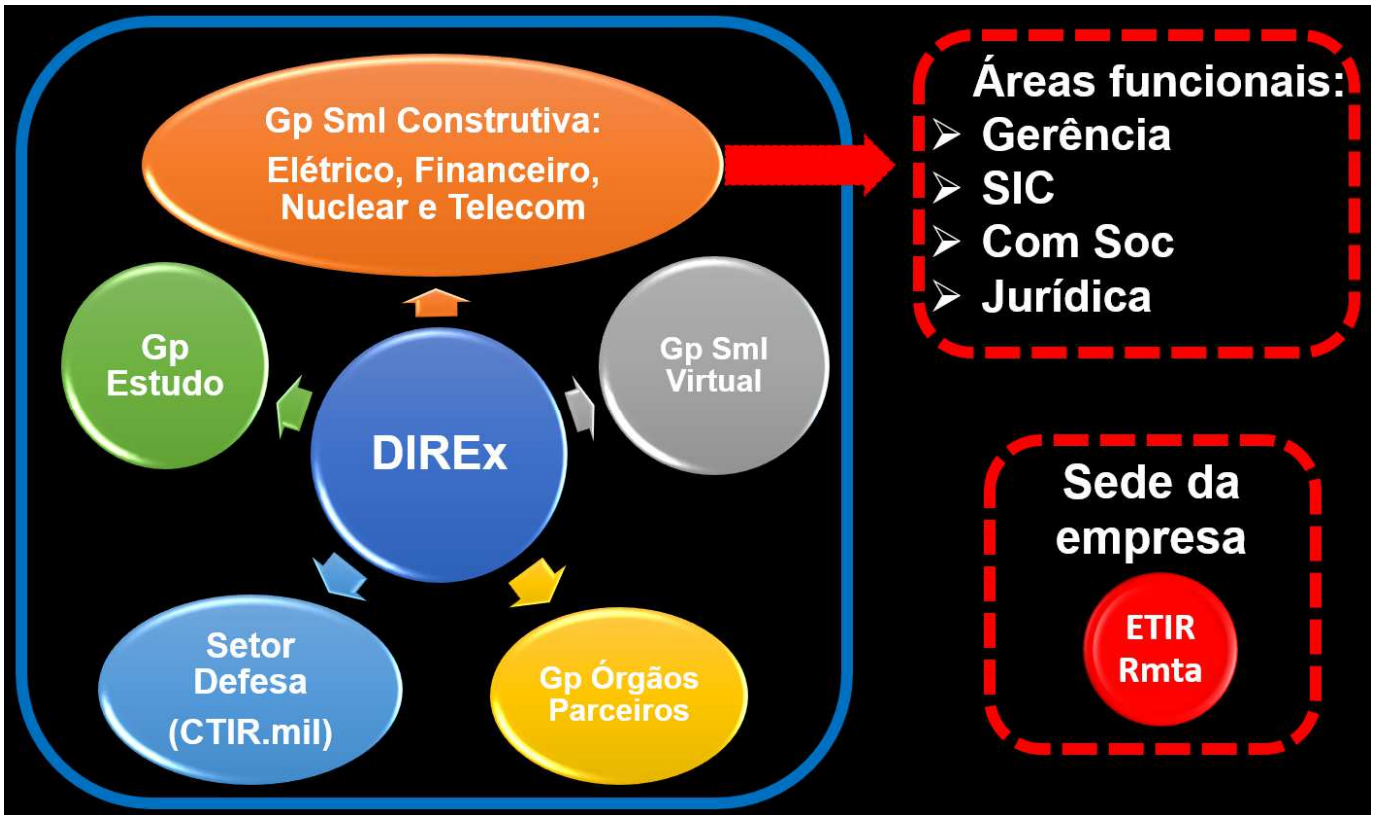
A simulação virtual teve o objetivo de identificar e difundir as melhores práticas das equipes de tratamento de incidentes de rede. A simulação construtiva permitiu exercitar o nível gerencial das organizações participantes na solução de problemas cibernéticos, por meio de ações envolvendo as áreas de segurança da informação, departamento jurídico e comunicação social.

Para envio e resposta dos problemas simulados a Direção do Exercício (DIREx) empregou como ferramenta o sistema de acompanhamento de eventos denominado *Request Tracker* (RT), o qual foi customizado pelo ComDCiber para uso no EGC 2.0.

A elaboração dos problemas simulados foi coordenada pelo Estado-Maior Conjunto (EM Cj) do ComDCiber em estreita ligação com as entidades centrais das organizações participantes nas diferentes áreas: Operador Nacional do Sistema Elétrico, Banco Central do Brasil, Departamento de Coordenação do Sistema de Proteção ao Programa Nuclear Brasileiro e Anatel.

Os representantes da Defesa Cibernética das Forças Armadas constituíram uma equipe conjunta para tratamento de incidentes de rede com atuação colaborativa do Centro de Tecnologia da Informação da Marinha, do Centro Integrado de Telemática do Exército e do Centro de Computação da Aeronáutica de Brasília.

Figura 1—Estrutura do EGC 2.0



Fonte: o autor (2019).

Empregou-se um cenário fictício de não-guerra, envolvendo as Forças Armadas e as áreas estratégicas de interesse para a Defesa Nacional.

Durante a execução do EGC 2.0 os incidentes foram apresentados de modo gradativo e intersetores, inclusive com o estabelecimento de um "Gabinete Nacional de Segurança Cibernética", para gerenciar as ações de Estado no ápice da crise do ambiente hipotético de conflito apresentado.

Os eventos simulados para os gabinetes de crise foram preparados durante o ciclo de planejamento, de modo conjunto e integrado com todos os envolvidos.

Para a elaboração dos eventos cibernéticos foram elencados temas nos quais poderiam ser desenvolvidas a interação intraempresa, intrasetor e intersetores.

A fim de facilitar a descrição dos eventos para o *table-top*, cada desafio proposto foi detalhado com base na resposta aos seguintes aspectos: o que, quando, quem, onde, por que, como e prejuízo gerado (5W2H). Foram preparadas soluções possíveis contendo: medidas reativas, medidas preventivas, bem como a interação entre os setores e organizações.

A seguir são descritas as principais áreas temáticas dos eventos simulados:

a) setor elétrico: estações de trabalho criptografadas por ransomware, envio de comandos indevidos para instalações, indisponibilidade de servidores Supervisory Control and Data Acquisition (SCADA), via ataques às instalações por distributed denial-of-service (DDoS), informações incorretas apresentadas nas consoles das salas de controle, engenharia social, indisponibilidade de redes de telecomunicações e vazamento de dados pessoais;

b) setor financeiro: indisponibilidade de estações e servidores Windows; transferências fraudulentas nos sistemas de pagamento interbancários; comprometimento da integridade dos sistemas de pagamento; e extorsão por vazamento de dados;

c) setor nuclear: ataque a instalações do ciclo de enriquecimento de combustível; vazamento de informações sensíveis; bem como comprometimento do sistema SCADA e de programmable logic controller (PLC);e

d) setor de telecomunicações: ataque do tipo Border Gateway Protocol (BGP).

Os cenários foram integrados de modo a permitir o uso da minuta do Plano Nacional de Tratamento de Incidentes de Redes, a fim de colher impressões para a sua posterior validação por parte do GSI/PR.

2.3 EMPREGO DO MALWARE INFORMATION SHARING PLATFORM (MISP)

Fruto de parceria com o Centro de Defesa Cibernética de Portugal, o ComDCiber está em fase de testes do MISP, ferramenta voltada para a troca de informações online sobre artefatos maliciosos amplamente utilizada pelos países da Organização do Tratado do Atlântico Norte (NATO, 2019).

O MISP é baseado em plataforma web, consistindo de uma comunidade voltada para o compartilhamento confiável de informações técnicas sobre malware com diferentes níveis de Traffic Light Protocol.

Trata-se da combinação multidirecional de repositórios com mecanismos para inserção e busca de dados. Permite a integração com Application Programming Interface (API) para produção de conhecimento e consciência situacional.

Uma de suas grandes vantagens é a rapidez com que permite registrar informações e contramedidas que podem ser adotadas para evitar que uma ameaça cibernética se propague.

Durante o EGC foram disponibilizadas contas de acesso à instância MISP do ComDCiber a todas as empresas e organizações participantes, o que permitiu apresentar a ferramenta e praticar o seu uso no âmbito das IEC.

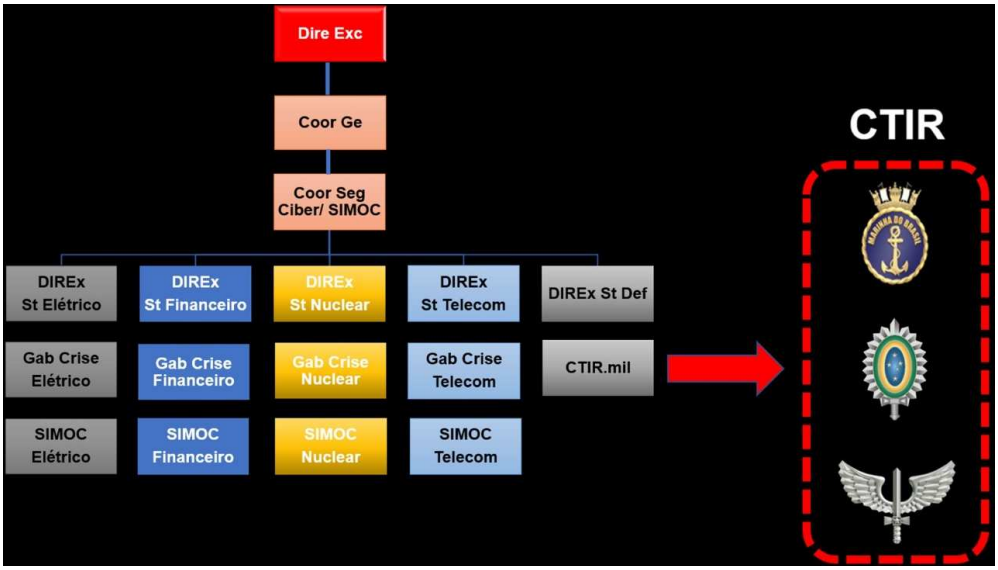
2.4 CONDUÇÃO DO EXERCÍCIO

A coordenação do EGC 2.0 foi realizada pelo ComDCiber em estreita ligação com os órgãos parceiros e empresas participantes.

A fim de facilitar os trabalhos, os órgãos centrais de cada área estratégica tiveram o encargo de capilarizar o planejamento, preparação e verificação das respostas aos incidentes simulados (Bacen, Anatel, DCSIPRON e ONS).

Foi adotada a seguinte organização das células de trabalho:

Figura 2—Estrutura do ECG 2.0



Fonte: o autor (2019).

2.4.1 Direção do exercício

Composta por integrantes de ComDCiber, CTIM, CITEx, CCA-BR, Cmdo Com GE Ex, bem como por 1(um) representante oriundo de cada empresa e organização participante.

2.4.2 Gabinetes de Crise – simulação construtiva (table-top exercise)

Células onde atuaram os participantes de nível gerencial das áreas estratégicas.

Cada empresa e organização participou com 1 (um) profissional oriundo de cada uma das seguintes áreas: gerência de segurança da informação, alta administração, comunicação social e assessoria jurídica.

Os problemas simulados gerados pela DIREx foram encaminhados para os gabinetes de crise por intermédio da ferramenta Request Tracker. Ao receberem os eventos as equipes tinham que apresentar as medidas reativas e preventivas, bem como a interação com as demais áreas estratégicas e órgãos parceiros, concluindo com a indicação de ensinamentos colhidos.

2.4.3 Grupo Órgãos Parceiros

Interagiram de modo colaborativo com as áreas estratégicas para a solução dos problemas simulados.

2.4.4 Grupo de Simulação Virtual

Foram empregados o Simulador de Operações Cibernéticas (SIMOC) e o Simulador de Planta Nuclear (SPN) para emulação de redes computacionais, a fim de identificar e corrigir vulnerabilidades.

Ressalta-se que a equipe do CIGE contou com o apoio de técnicos do SERPRO para a criação de cenários cibernéticos no SIMOC.

Cada empresa e organização convidada participou com 1 (um) especialista de nível técnico operando os cyber ranges citados.

O SPN em sua versão inicial foi desenvolvido pelo CTMSP em parceria com a AIEA e foi empregado pela primeira vez durante o EGC. Contou com a presença de observador internacional oriundo da referida agência e permitiu avaliar o impacto de ataques cibernéticos sobre instalação nuclear.

2.4.5 Grupo Defesa

Atuou de forma conjunta e integrada, constituindo um Centro de Tratamento de Incidentes de Redes Militar.

Respondeu a eventos que tiveram origem sobre as IEC e que geraram efeitos sobre o nível de operacionalidade das Forças. Como exemplos:

a) ataque cibernético sobre data center em provedor de telecomunicações afetou a velocidade de conexão das infovias, degradando a operação do Sistema de Monitoramento de Fronteiras;

b) ramsonware em redes computacionais do sistema financeiro impediu que a Defesa emitisse ordens bancárias para o pagamento de prestadoras de serviços, prejudicando a manutenção do material de emprego militar;

c) instabilidade no sistema SCADA de controle das linhas de transmissão prejudicou o fornecimento de energia elétrica a organizações militares estratégicas para a Defesa Nacional.

2.5 WORKSHOP SOBRE GESTÃO DE RISCO CIBERNÉTICO

Durante a fase de preparação do EGC, na Reunião Final de Coodenação, foi realizado o 1º Workshop em Gestão de Riscos Cibernéticos, contando com a presença de especialistas norte-americanos do *National Institute of Standards and Technology* (NIST).

Estes *experts* apresentaram o *Cybersecurity Framework* e participaram dos estudos nas salas temáticas dos setores elétrico, financeiro, nuclear e de telecomunicações abordando os seguintes temas:

a) gestão de Riscos da Segurança Cibernética das Infraestruturas Críticas;

b) indicadores e pontos de controle para as IEC que podem ser utilizados por órgãos de governo;

c) estrutura para processos de identificação dos ativos que, se atacados, geram maior impacto;

d) análise de riscos e proposição de planos de ação para cada setor estratégico;

e) privacidade de dados e liberdade civil;

f) *benchmarking* de programas de gerenciamento de riscos cibernéticos implementados pelas empresas;e

g) como aplicar o Framework do NIST nos diferentes setores estratégicos e principais dificuldades para implementação.

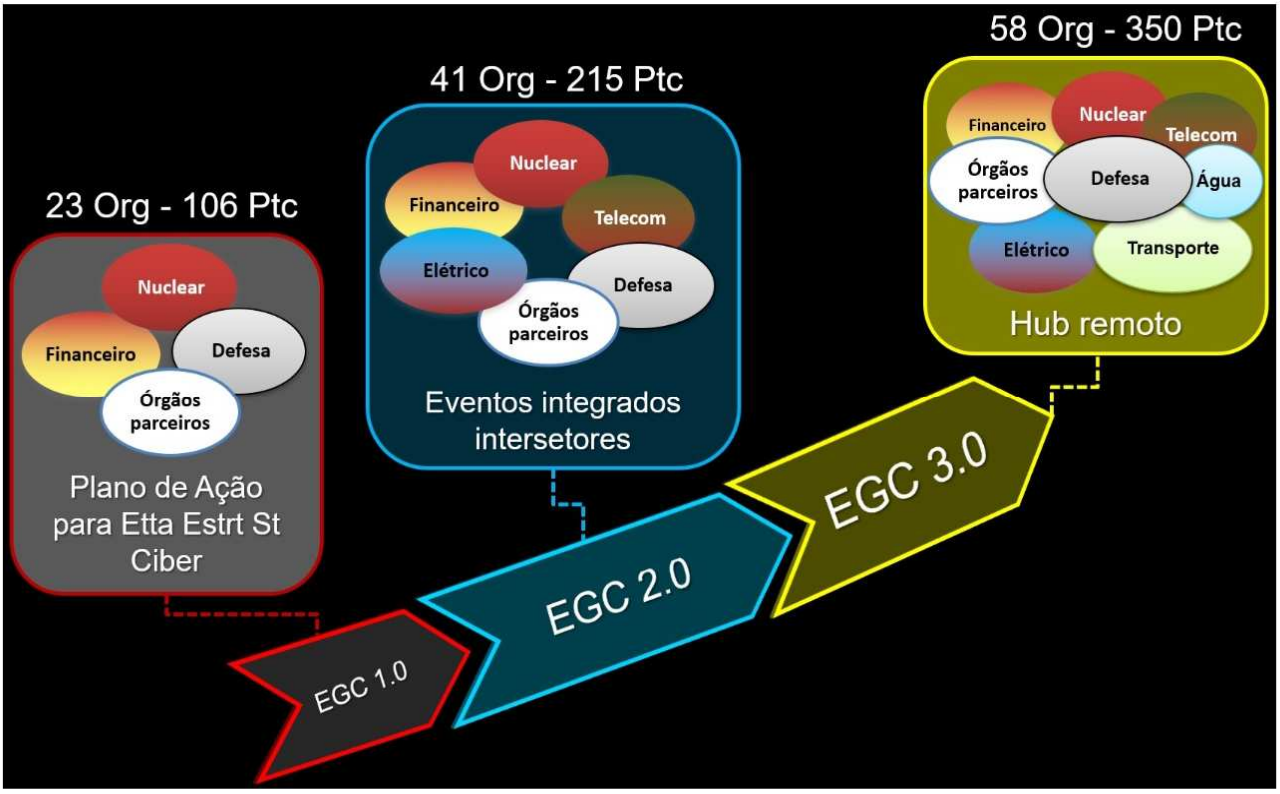
2.6 EVOLUÇÃO DO EGC PARA a 3ª EDIÇÃO

Quadro 2 - Principais aspectos de evolução do ECG 3.0

Linha de Esforço	Evolução
Simulações Virtual e Construtiva	Inserção dos setores de Água e Transporte Aéreo nas simulações virtual e construtiva
	Prática de incidentes relacionados aos "Desafios da Próxima Década", envolvendo inteligência artificial, telefonia móvel 5G e ataques a redes de cabos submarinos
	Estabelecimento de um *hub* remoto em São Paulo com estrutura de DIREx, bem como de ambientes para simulações virtual e construtiva
	Emprego da 2ª versão do Simulador de Planta Nuclear mediante cooperação com a Agência Internacional de Energia Atômica e com o CTMSP
Grupo de Estudo	Workshop sobre ações estratégicas no Setor Cibernético
	"Dia do Engajamento Ciber" com apresentações nas empresas sobre *Cyber Hygiene*
Cooperação Internacional	Parceria com o CCDCOE para emprego do Cenário 3 da ferramenta *Cyber Law Toolkit*, relacionado às implicações legais na proteção cibernética de infraestruturas críticas

Fonte: o autor (2019).

Figura 3 - Evolução do EGC



Fonte: o autor (2019).

3 CONCLUSÃO

O domínio cibernético perpassa a sociedade como um todo, provendo suporte para a economia global, infraestruturas críticas, segurança pública e defesa nacional, não respeitando fronteira física entre as nações.

Trata-se de um desafio que necessita de soluções estratégicas de longo prazo, requerendo ampla cooperação por meio do envolvimento de países, organismos internacionais, governo, Forças Armadas, comunidade acadêmica e setor privado.

O formato adotado no EGC contribui para incrementar a resiliência cibernética, por meio do estímulo à unidade de esforço entre os diversos atores civis e militares que constituem o ecossistema cibernético (EXÉRCITO BRASILEIRO, 2019b).

Como ensinamentos colhidos, destacam-se:

a)necessidade da rapidez e da oportunidade no compartilhamento de informação para fazer frente ao dinamismo e às incertezas das ameaças cibernéticas;

b) importância da troca permanente de experiências relacionadas às boas práticas*;*

c) conhecimento mútuo acerca das possibilidades e limitações dos diversos *stakeholders* que integram o espaço cibernético;

d) importância da Estratégia Nacional de Segurança Cibernética para a integração de iniciativas, alinhamento normativo e amadurecimento da sociedade quanto ao tema; e

e) identificação de subsídios para a melhoria do Plano Nacional de Tratamento de Incidentes de Redes.

Por fim, o EGC tem evoluído ao longo de suas edições, buscando agregar novos atores e reforçar a sinergia entre os envolvidos. O exercício representa a materialização da cooperação e integração entre o Sistema Militar de Defesa Cibernética e a proteção de infraestruturas críticas de interesse para a Defesa Nacional.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Livro Verde da Seguran**ça Cibernética. Brasília, DF: GSI, 2010.

_____. Gabinete de Segurança Institucional da Presidência da República. **Estratégia de Segurança da Informação e** Comunicações e de Segurança Cibernética da Administração Pública Federal. Brasília, DF: GSI, 2015.

_____. Gabinete de Segurança Institucional da Presidência da República. **Política Nacional de Segurança da Informação**. Brasília, DF: GSI, 2018.

_____. Gabinete de Segurança Institucional da Presidência da República. **Estratégia Nacional de Segurança Cibernética**. Disponível em: http://participa.br/seguranca-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber. Acesso em 10 de outubro de 2019.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, DF: Diário Oficial da União, 2008.

_____. Ministério da Defesa. **Diretriz do Ministério da Defesa Nr 14, Integração e Coordenação dos Setores Estratégicos de Defesa**. Brasília, DF: MD, 2009.

_____. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética (MD31-M-07)**. Brasília, DF: MD, 2014.

CCDCOE. **Cyberlaw Toolkit.** Disponível em: https://cyberlaw.ccdcoe.org/wiki/Scenario_03:_Cyber_operation_against_the_power_grid. Acesso em 10 de outubro de 2019.

E-ISAC. **Electricity Information Sharing and Analysis Center.** Analysis of the Cyber Attack on the Ukrainian Power Grid**.** Washington D.C., EUA: E-ISAC, 2016.

EXÉRCITO BRASILEIRO**. Noticiário do Exército sobre o Exercício Guardião Cibernético 2.0**. Disponível em: http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/id/9007697. Acesso em 10 de outubro de 2019a.

_____. Vídeo (4 min) do Exercício Guardião Cibernético 2.0. Disponível em: https://www.youtube.com/watch?v=a30GvHuYD64. Acesso em 10 de outubro de 2019b.

_____. **Guerra Cibernética (EB70-MC-10.232)**. Brasília, DF: EB, 2017.

NATO. Communications and Information Agency. **Malware Information Sharing Platform Leaflet**. Bruxelas, Bélgica, 2019.

*Tenente-Coronel **WALBERY** NOGUEIRA DE LIMA E SILVA é oficial de Estado-Maior do Comando de Defesa Cibernética e desempenhou a função de Coordenador Executivo do Exercício Guardião Cibernético (walbery.nogueira@eb.mil.br). Artigo realizado como trabalho de conclusão do Curso de Especialização em Planejamento de Guerra Eletrônica e Guerra Cibernética em Apoio às Operações, do Centro de Instrução de Guerra Eletrônica.

DATA & HERTZ

Centro de Instrução de Guerra Eletrônica (CIGE)
Seção de Pós-graduação (SPG)