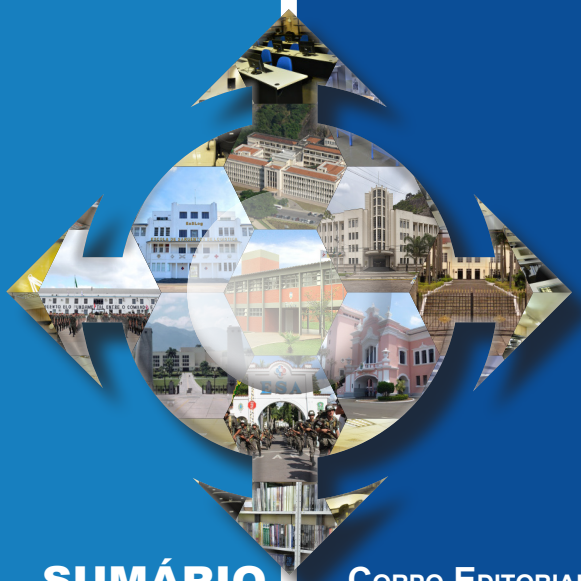
ISSN 2594-3952



O Comunicante

SUMÁRIO

Artigos

Revista Científica da Escola de Comunicações

Escola Coronel Hygino Corsetti

VOLUME 9 - Nº 1

Fevereiro 2019

ISSN 2594-3952

O Comunicante

SUMÁRIO

Artigos

Revista Científica da Escola de Comunicações

Escola Coronel Hygino Corsetti

VOLUME 9 - Nº 1

Fevereiro 2019

O COMUNICANTE
Revista Científica da Escola de Comunicações

Ano 9 - Nº 1

Fevereiro 2019

ISSN 1968-6029

ISSN 2594-3952 (Digital)

Escola de Comunicações - EsCom

Escola Coronel Hygino Corsetti

EDITORIAL

A presente Edição da Revista "O Comunicante" apresenta os trabalhos científicos submetidos durante a II Conferência Científica em Assuntos de Defesa (CICAD), conduzida por esta Escola no mês de novembro de 2018, no Auditório da Fundação Habitacional do Exército, em Brasília. Os temas apresentados englobam as áreas de concentração de telecomunicações, tecnologia da informação, cibernética e educação. Todos esses temas são relevantes para atividade de Defesa Nacional, mais especificamente para o exercício de Comando e Controle em operações militares.

Sobre o campo cibernético, observa-se o interesse cada vez maior dos novos pesquisadores pelo tema, o que demonstra a potencialidade deste campo de estudos e sua aplicabilidade ao campo militar. Sintonizado com essa necessidade, a EsCom tem estimulado o desenvolvimento do assunto, promovendo aperfeiçoamentos na grade curricular dos cursos que ministra.

Destaca-se, ainda, o trabalho apresentado pelo Maj Ricardo Inacio Dondoni, que buscou traçar as novas necessidades cognitivas para o desempenho das competências nas atividades relacionadas ao emprego dos meios de comunicações, contribuindo para o debate em torno da necessidade de se construir uma trilha do conhecimento para os profissionais que ingressam nas especialidades de comunicações, guerra eletrônica e cibernética no Exército Brasileiro.

Ressalta-se a participação de alunos e pesquisadores oriundos de instituições de ensino civis, o que permite o intercâmbio de ideias, alinhada com as diretrizes do sistema de educação e cultura do Exército Brasileiro e com a Estratégia Nacional de Defesa.

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

Uma boa leitura a todos.

RODOLFO ROQUE SALGUERO DE LA VEGA FILHO - Cel
Comandante da Escola de Comunicações

EXPEDIENTE

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

OBJETIVOS

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

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

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

Publicar artigos inéditos e de qualidade.

Aprofundar pesquisas e informações sobre assuntos da atualidade em proveito da Defesa e difundir aos Corpos de Tropa.

PÚBLICO-ALVO

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

PUBLICAÇÃO DE ARTIGOS

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

PROCESSO DE AVALIAÇÃO

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

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

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

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

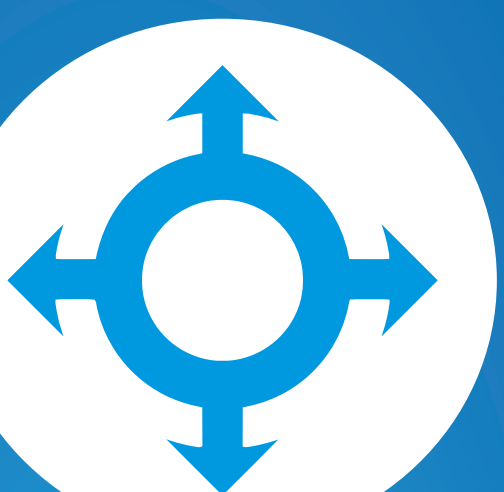
PERIODICIDADE

A revista tem periodicidade quadrimestral (fevereiro, junho e outubro) e se reserva ao direito de realizar edições especiais, além das previstas.

O Comunicante - Revista Científica da Escola de Comunicações - Volume 9, Nº 1(Fev/2019)
Brasília-DF: Escola de Comunicações. 2019 72p; 29,7 cm X 21,0 cm

Publicação Quadrimestral
ISSN 1968-6029 ISSN 2594-3952(Digital)
Revista Científica da Escola de Comunicações
1. Escola de Comunicações 2. Defesa 3. Cibernética 4. Ciência & Tecnologia 5. Doutrina 6. Direito 7. Educação 8. Informática 9. Instrução Militar 10. Gestão 11. Meio Ambiente 12. Operações Militares Conjuntas e Singulares.

Orientadores dos Artigos publicados



Edson Benício de Carvalho Júnior

- Doutorado em Transportes.
- Pesquisador e professor nos cursos de Engenharia Civil.
- UCB e UniCEUB

http://lattes.cnpq.br/7032871098900569

Jorge Madeira Nogueira

- Doutorado em Desenvolvimento Agrário
- Professor Titular do Departamento de Economia da Universidade de Brasília (ECO/UnB).
- UnB

http://lattes.cnpq.br/1869009681242978

CICAD.II.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

AVALIAÇÃO DO IMPACTO DO RUÍDO AERONÁUTICO NO ENTORNO DE BRASÍLIA

Raphaella de Souza Serapião Amorim, Patrícia dos Reis de Morais
Graduanda em Engenharia Civil, Graduanda em Engenharia Civil

RESUMO: O presente estudo avaliou o impacto do ruído aeronáutico, no entorno do Aeroporto Internacional de Brasília, após a implementação das operações simultâneas nas suas quatro cabeceiras. Tornou-se, assim, o primeiro aeroporto da América do Sul a operar com as cabeceiras independentes. Para tanto, foram elaboradas curvas de ruído com dados fornecidos pela INFRAMERICA. As isofônicas foram simuladas no softwares INM 7.0d com base na metodologia descrita no Regulamento Brasileiro da Aviação Civil 161 (2013). A métrica acústica adotada foi o DNL (day-night average sound level). Também foi utilizada uma ferramenta SIG para elaboração dos mapas de ruído. Foram realizadas simulações para dois cenários. O primeiro para março de 2017, onde ocorreram operações de pouso e decolagem no formato padrão (com movimentações de pouso ocorrendo preferencialmente em uma pista e as de decolagem em outra). O segundo cenário foi para março de 2018 onde ocorreram somente operações simultâneas nas quatro cabeceiras. O total de movimentações foi de 13.366 (2017) e 13.260 (2018) movimentações/mês. Com base nas curvas de ruído geradas, não se observou mudanças expressivas dentre os cenários em relação ao ruído aeronáutico nas áreas circunvizinhas ao Aeroporto. Todavia, verificou-se uma população exposta significativa ao ruído aeroviário nas DNL's 55 e 60 (fora das restrições de uso e ocupação do solo indicados no RBAC 161) que atingem regiões de Taguatinga, Samambaia, Riacho Fundo, Setor de Mansões Dom Bosco e Lago Sul. Apesar de serem compatíveis com o uso residencial, o ruído aeronáutico nessas regiões é percebido pelos moradores podendo gerar reações.

Palavras-chave: Ruído aeronáutico. Zoneamento Sonoro. Mapas de ruído. Impacto ambiental.

INTRODUÇÃO

Os aeroportos tornaram-se um componente vital da infraestrutura de transporte das cidades modernas, exercendo cada vez mais influência no zoneamento urbano. Entretanto, aeroportos também são responsáveis por importantes externalidades ambientais destacando-se os efeitos nocivos à saúde humana causados pelo ruído, tais como: incômodo, hipertensão, problemas cardíacos, psicológicos, emocionais, estresse e males associados a distúrbios no sono (BABISCH, W. 2002; JARUP et al., 2005; HARALABIDIS A. S. et al., 2008; BABISCH, W. et al., 2009).

O ruído aeronáutico também exerce uma influência negativa na percepção de bem-estar e satisfação das pessoas em residirem em uma determinada região da cidade (KROESEN, M. et al., 2010). Isso contribui para desenvolvimento de conflitos entre os principais atores envolvidos em áreas de aeroportos, ou seja, operadores, governos locais e comunidade (FABUREL, 2005 e DE BARROS A. G., 2013).

Vale ainda ressaltar que os efeitos adversos sobre o sono se tornaram uma das queixas mais comuns apontadas por populações expostas ao ruído na Europa (WHO, 2009). Também se associa ao ruído aeroviário impactos de ordem econômica e social. Propriedades próximas a um aeroporto vêm sofrendo crescente depreciação relacionada ao aumento do ruído aeroportuário (FEITELSON et al., 1996; MORRELL and LU, 2000; NAVRUD, 2002; NELSON, 2004; BROOKER, 2006; DEKKERS e STRAATEN, 2009; PUCHELL e EVANGELINOS, 2012; MATOS et al., 2013).

O Grupo de Pesquisa em Acústica e Poluição Ambiental, proponente deste projeto, ressalta que região afetada pelo ruído aeronáutico, no entorno do Aeroporto de Brasília, sofreu alterações em virtude da nova operação nesse aeroporto a partir do ano de 2016. O Departamento de Controle do Espaço aéreo (DECEA) autorizou o crescimento da capaci-

dade desse aeroporto, com intuito de aumentar a quantidade de voos por dia com as suas duas pistas e quatro cabeceiras (29R/11L e 29L/11R) operando simultaneamente de forma independente. Assim, a movimentação de aeronaves passou de 60 movimentos aéreos/hora para 80 aéreos/hora, sendo o primeiro aeroporto da América do Sul a operar com quatro cabeceiras simultaneamente.

No Brasil, os conflitos associados ao ruído aeronáutico fazem parte da realidade cotidiana de grandes cidades. Por exemplo, é o caso de as comunidades vizinhas ao Aeroporto Internacional de Congonhas, em São Paulo, que incomodadas com o ruído dos aviões, manifestaram-se contra o aumento do tráfego aéreo levando ao fechamento noturno do aeroporto. Segundo Carvalho Jr, E. (2015), o Brasil ainda carece de estudos que busquem verificar os efeitos negativos do ruído aeronáutico na qualidade de vida das comunidades afetadas. É nesse ponto que reside a contribuição científica do presente projeto, ou seja, sustenta-se na necessidade do desenvolvimento de pesquisas que contribuam para uma melhor compreensão do impacto causado pelo ruído aeroviário em regiões no entorno de aeroportos. Cabe ressaltar que o estudo aqui proposto é inédito para a atual operação do Aeroporto Internacional de Brasília e servirá como parâmetro para estudos em outras cidades brasileiras.

1 FUNDAMENTAÇÃO TEÓRICA

1.1 O RUÍDO AERONÁUTICO

O ruído aeronáutico é todo ruído produzido por aeronaves em operação de pouso, decolagem, taxiamento, circulação e testes de motores. Considera-se, ainda, o ruído produzido pelos equipamentos auxiliares a aeronaves. Uma das particularidades do ruído aeronáutico é que este, além de afetar seu entorno imediato, pode vir a influenciar áreas relativamente distantes de seu espaço físico, isto porque a principal fonte de ruído, a aeronave, ultrapassa os limites dos aeroportos sobrevoando muitas vezes áreas densamente povoadas (ROCHA e SLAMA, 2008).

O ruído aeroportuário é caracterizado por ter vários picos de energia sonora, não sendo, portanto, ouvido o tempo todo. As diversas fontes sonoras provenientes das atividades aeroportuárias, às quais as comunidades próximas ao aeroporto estão expostas, não são estacionárias com relação ao tempo. Além disso, o ruído aeroviário ocorre, na maioria dos casos, em baixa frequência, ocasionando os mais diversos efeitos sobre o público exposto a ele. Esse fenômeno atinge, sobretudo, as pessoas que residem em locais próximos aos aeroportos, influenciando diretamente na qualidade de vida dessa parcela da população. Vale ressaltar que os momentos em que ocorre maior intensidade do ruído correspondem aos pousos, decolagens e sobrevoos (HELENO, 2010).

A intensidade do ruído produzido por aeronaves a jato é muito maior do que as intensidades de ruídos provenientes de outras fontes do cotidiano das cidades. Outra característica importante a ressaltar é o fato da fonte de ruído ser móvel e estar acima do nível do solo durante a maior parte do tempo, o que facilita a propagação do som pela falta de obstáculos (IAC 4102, 1981).

Especificamente, o efeito do ruído aeronáutico no sono é uma preocupação há muito tempo reconhecida pelos estudiosos interessados em determinar o impacto do ruído sobre as pessoas (FICAN, 1997). Geralmente, os modais de transportes no período noturno, são as principais fontes de ruído, sendo que devido à sua natureza intermitente, o ruído das aeronaves é considerado o que produz maior incômodo (JONES, 2009).

Clark e Stansfeld (2011), em uma recente revisão da literatura, a respeito do ruído aeronáutico no período noturno e os efeitos na saúde, concluíram que a exposição ao ruído aeroviário noturno está potencialmente associado a impactos na saúde pública e na qualidade de vida dos moradores que vivem

perto de grandes aeroportos. Também verificaram que existem robustas evidências de que os efeitos à exposição noturna ao ruído aeronáutico estão relacionados com hipertensão, distúrbios do sono e incômodo sonoro. Ainda destacam que essas evidências são suficientes para apoiar medidas de prevenção, tais como diretrizes políticas e o estabelecimento de valores limites à exposição noturna ao ruído aeroviário em comunidades próximas a aeroportos (CLARK; STANSFELD, 2011)

O ruído aeroviário provoca efeitos nocivos à saúde humana, tais como: incômodo, hipertensão, problemas cardíacos, psicológicos, emocionais, estresse e males associados a distúrbios no sono (BABISCH, 2002, JARUP et al., 2005; HARALABIDIS et al., 2008, BABISCH et al., 2009). Ressalta-se que os efeitos adversos sobre o sono se tornaram uma das queixas mais comuns apontadas por populações expostas ao ruído na Europa (WHO, 2009).

Cabe ressaltar que, nas últimas décadas, ocorreu uma evolução tecnológica dos motores utilizados pelos aviões o que implicou na redução dos níveis de ruído gerado individualmente por cada aeronave. Além disso, os limites de ruído externos para certificação de aeronaves tornaram-se mais restritivos (BONATTO, 2013). Todavia, embora a evolução das aeronaves tenha reduzido o nível de ruído produzido por cada uma delas, o ruído aeroportuário teve forte elevação devido ao grande aumento no número de operações aeronáuticas desde a década de 1950 até os dias atuais (ROCHA e SLAMA, 2008).

Dessa forma, o ruído das aeronaves tornou-se um dos principais problemas relacionados à atividade aeroportuária, pois comunidades expostas podem desencadear reações capazes de ocasionar importantes restrições à capacidade operacional, à expansão e até à construção de novos aeroportos (GIRVIN, 2009; SUAU-SANCHEZ et al., 2011; DE BARROS, 2013; SADR MK et al., 2014). Por exemplo, é o caso das comunidades vizinhas ao Aeroporto Internacional de Congonhas, em São Paulo, que incomodadas com o ruído dos aviões, manifestaram contra o aumento do tráfego aéreo levando ao fechamento noturno do aeroporto. Do exposto, fica destacada a importância de se realizar estudos capazes de satisfazer não só a demanda pelo transporte aéreo, mas também viabilizar o desenvolvimento de medidas que minimizem o impacto do ruído na saúde e na qualidade de vida das comunidades expostas.

1.2 CURVAS DE RUÍDO E INDICADOR ACÚSTICO

O Regulamento Brasileiro da Aviação Civil (RBAC) N° 161 de 2013 define curvas de ruído como sendo linhas traçadas em um mapa, cada uma representando níveis iguais de exposição ao ruído. Também estabelece que as curvas de ruído deverão ser calculadas por meio de programa computacional que utilize metodologia matemática apropriada para a geração de curvas na métrica DNL (Day-night level), considerando como período noturno o período compreendido entre 22h e 7h do horário local.

O DNL é uma medida cumulativa da energia total do som e representa uma média logarítmica dos níveis sonoros durante um período de 24 horas, com uma penalização de 10 dB adicionado a todos os sons que ocorram durante o horário noturno (das 22h às 7h). A pena de 10 dB representa a intromissão do ruído adicionado à noite, pois os níveis de som ambiente durante as horas noturnas são, tipicamente cerca de 10 dB inferiores aos níveis medidos durante o dia, e por causa da irritação associada a distúrbios do sono (CARVALHO JR, E et al, 2013; FAA, 2011).

De acordo com a NBR 11.415 (ABNT, 1990), o nível de incômodo sonoro medido pelo método DNL é determinado pelo Leq para 24h, sendo que no período das 22h às 7h, somam-se 10 dB a todos os níveis medidos. É definido da seguinte forma:

$$DNL = 10 \times \log\left[\frac{1}{24}\left(15 \times 10^{\frac{L_d}{10}} + 9 \times 10^{\frac{(L_n+10)}{10}}\right)\right] \quad (1)$$

Onde o número 24 corresponde às horas medidas, 15 ao período diurno e 9 ao noturno, sendo que o período noturno deve começar depois das 22h e não deve terminar antes das 7h do dia seguinte. Já Ld corresponde ao Leq para o período diurno e Ln ao Leq para o noturno. Já o nível de pressão sonora equivalente (Leq), ou nível contínuo equivalente, é o som produzido durante um dado período de tempo, é expresso em dB e calculado de acordo com a NBR 10.151 (ABNT, 2000) pela equação 2:

$$L_{eq} = 10 \times \log_{10}\left(\frac{1}{T}\int_0^T \frac{p(t)^2}{p_0^2}dt\right) \quad (2)$$

Onde T é a duração do período de referência (tempo total de medida); p(t) é a pressão sonora instantânea; p0 é pressão sonora de referência (2,0 x 10^{-5} N/m2). A Equação 2 mostra que o nível equivalente é representado por um valor constante que durante o mesmo tempo T, resultaria na mesma energia acústica produzida pelos valores instantâneos variáveis de pressão sonora.

O RBAC 161 (213) estabelece ainda que para aeródromos com média anual de movimento de aeronaves dos últimos 3 (três) anos superior a 7.000 (sete mil), deve ser elaborado um estudo com cinco curvas de ruído conforme indicado a seguir:

- Curva de Ruído de 85 é a linha traçada a partir da interpolação dos pontos que apresentam nível de ruído médio dia-noite de 85 dB.
- Curva de Ruído de 80 é a linha traçada a partir da interpolação dos pontos que apresentam nível de ruído médio dia-noite de 80 dB.
- Curva de Ruído de 75 é a linha traçada a partir da interpolação dos pontos que apresentam nível de ruído médio dia-noite de 75 dB.
- Curva de Ruído de 70 é a linha traçada a partir da interpolação dos pontos que apresentam nível de ruído médio dia-noite de 70 dB.
- Curva de Ruído de 65 é a linha traçada a partir da interpolação dos pontos que apresentam nível de ruído médio dia-noite de 65 dB.

2 METODOLOGIA

O método foi sustentado em simulações de curvas de ruído e elaboração de mapas de ruído. Para a simulação foi utilizada a metodologia descrita no Regulamento Brasileiro da Aviação Civil 161 de 2013 com uso da métrica acústica DNL (day-night average sound level) que representa o nível de ruído médio em um período de 24h. O software utilizado foi o Integrated Noise Model (INM), desenvolvido pelo FAA (Federal Aviation Administration – EUA).

O INM foi projetado para realizar modelagens dinâmicas e alta performance relacionadas ao ruído aeronáutico. Com relação ao ruído, o INM permite estimar os efeitos médios de longo prazo utilizando um input baseado em uma média anual de operações de um aeroporto. O output gerado foi exportado para um software SIG para elaboração dos mapas de ruído. Os dados necessários para a realização da pesquisa foram fornecidos pela operadora do aeroporto – INFRAMERICA.

2.1 CARACTERIZAÇÃO DO AEROPORTO INTERNACIONAL DE BRASÍLIA

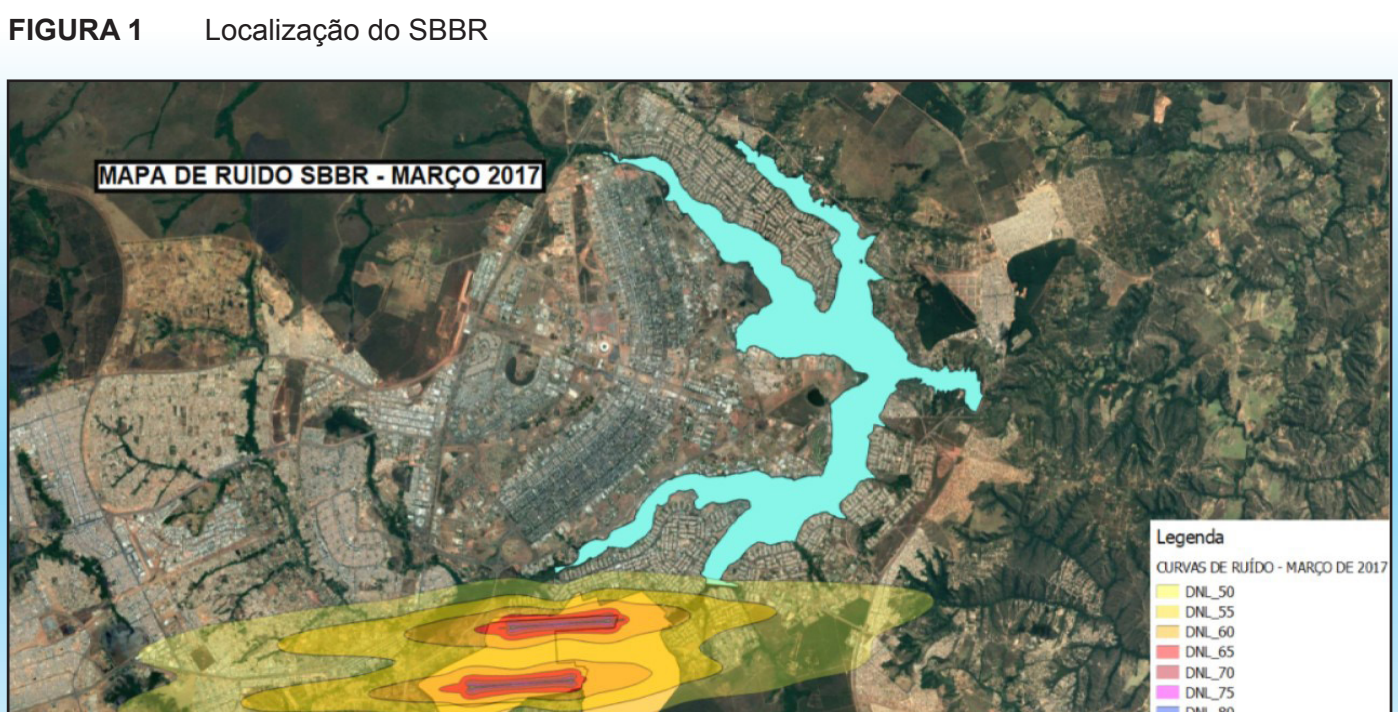
O Aeroporto Internacional de Brasília possui sigla ICAO (International Civil Aviation Organization) SBBR. Atualmente, é o segundo em movimentação de aeronaves e de passageiros no Brasil e que devido sua localização geográfica, recebe e distribui mais de 500 voos por dia, sendo considerado ponto de conexão para destinos em todo o país, e no exterior. A crescente demanda por operações nesse aeroporto e sua proximidade com áreas residenciais apontam para uma situação de comprometimento do ambiente sonoro de seu entorno com significativo potencial de incômodo (CARVALHO JR et al., 2012).

O sítio aeroportuário do Aeroporto In-

ternacional de Brasília (SBBR) possui área total de 28.930.886 m². Trata-se de um aeroporto compartilhado, isto é, com operações civis e militares. A área militar é de 18.977.685 m² e a área patrimonial civil de 9.947.559 m². Na Figura 1 é possível observar o sítio aeroportuário e as áreas destinadas ao uso civil e ao uso militar. Em sua infraestrutura física, o SBBR possui vias de acesso, estacionamentos, área de apoio, hangares, pátio de manobras, pista de taxiamento, pista de pouso e decolagem e terminal de passageiros com estabelecimentos comerciais e área administrativa, técnica e de passageiros e área de terminal de cargas. Possui também instalações militares na área militar da Base Aérea de Brasília.

Desde 1º de março de 2013, a INFRAMÉRICA assumiu a operação do Aeroporto de Brasília, ficando responsável pela operação comercial e pela gestão, manutenção e funcionamento de todos os serviços básicos. Está também a cargo da INFRAMÉRICA a segurança, a vigilância, a operação e a manutenção de todo o sítio aeroportuário, parte civil (BSBAERO, 2013).

FIGURA 1 Localização do SBBR



Fonte: Carvalho Jr. E, 2015.

2.2 DADOS DE OPERAÇÃO UTILIZADOS NAS SIMULAÇÕES

Foram realizadas simulações para dois cenários. O primeiro para o mês de março de 2017 onde ocorreram operações de pouso e decolagem no formato padrão, ou seja, as movimentações de pouso ocorrem preferencialmente em uma pista e as de decolagem na outra pista. O segundo cenário foi para março de 2018 onde ocorreram somente operações simultâneas nas duas pistas do SBBR. O mês de março foi definido pelo operador aeroportuário (INFRAMÉRICA), por ser um mês em que ocorreram somente operações do tipo padrão em 2017 (cenário 1) e somente operações simultâneas em 2018 (cenário 2).

Para a simulação das curvas de ruído são necessários vários dados de entradas tais como: elevação, velocidade média anual do vento, temperatura média anual de referência etc. Esses dados devem ser obtidos em fontes oficiais do governo ou com a própria empresa operadora do aeroporto. A Tabela 1 apresenta esses dados obtidos no sítio do Departamento de Controle do Espaço Aéreo (DECEA – AIM) e junto à INFRAMÉRICA, empresa operadora

do SBBR.

TABELA 1 Dados gerais do SBBR

Operador Aeroportuário	INFRAMÉRICA
Cidade	Brasília
Elevação do aeródromo	1066 m
Velocidade média do vento	15 km/h
Designador ICAO	SBBR
Coordenadas Geográficas	47º 54' 55" W / 15º 51' 38" S
Estado	Distrito Federal (DF)
Temperatura de referência	30º C

Fonte: o autor, 2018.

Já a Tabela 2 resume os dados das pistas do SBBR que constam da Carta do Aeródromo SBBR. De acordo com a NBR 10.151 (ABNT, 2000), o período noturno foi considerado entre 22 h e 7 h do dia seguinte, o diurno foi considerado entre 7 e 22 horas. As Tabelas 3 e 4 mostram o percentual de operações de pousos e decolagens, em cada cabeceira do SBBR, com base nos meses de março 2017 e 2018. Os dados que constam dessas tabelas foram sintetizados do histórico de operação enviado pela INFRAMERICA .

TABELA 2 Dados da pista

Pista	Comprimento	Cabeceiras			
		Cabeceira	Altitude	Latitude	Longitude
11L / 29R	3.200 m	11L	1051	15º 51' 49" S	47º 55' 39" W
		29R	1060	15º 51' 42" S	47º 53' 52" W
11L / 29L	3.300m	11R	1066	15º 52' 50" S	47º 56' 24" W
		29L	1042	15º 52' 43" S	47º 54' 33" W

Fonte: o autor, 2018.

TABELA 3 Operações de pouso e decolagem - SBBR (março de 2017)

Cabeceira	Pouso	% Pouso	Decolagem	% Decolagem	Total	% Total
11 L	2575	39%	2164	32%	4739	35,5 %
29 R	761	11%	470	7%	1231	9,2 %
11 R	2569	39%	3132	47%	5701	42,7 %
29 L	764	11%	931	14%	1695	12,7 %
Total	**6669**	**1**	**6697**	**1**	**13366**	

Fonte: o autor, 2018.

TABELA 4 Operações de pouso e decolagem - SBBR (março de 2018)

Cabeceira	Pouso	% Pouso	Decolagem	% Decolagem	Total	% Total
11 L	2085	31 %	1544	24 %	3629	27,4 %
29 R	1109	16 %	953	15 %	2062	15,6 %
11 R	2121	31 %	2613	40 %	4734	35,7 %
29 L	1423	21 %	1412	22 %	2835	21,4 %
Total	**6738**	**1**	**6522**	**1**	**13260**	

Fonte: o autor, 2018.

As Tabelas 5 e 6 expressam os percentuais de operação para o período diurno e noturno dos meses de março de 2017 e 2018. As Tabelas 7 e 8 apresentam a frequência e os percentuais de operação (pouso e decolagem) de cada uma das cabeceiras para o período diurno e noturno nos meses de março de 2017 e 2018. Esses dados são essenciais para simulação das curvas de ruído no INM 7.0 d.

TABELA 5 Percentuais de operações diurno e noturno (março 2017)

Operação Noturna	Freq	% op
Pouso	764	51,0 %
Decolagem	735	49,0 %
Total Op. Noturna	1499	11,2 %
Operação Diurna	**Freq**	**% op**
Pouso	5905	49,8 %
Decolagem	5962	50,2 %
Total Op Diruna	11867	88,8 %
Total Pouso	6669	49,9 %
Total Decolagem	6697	50,1 %
Total Pouso + Decolagem	13366	

Fonte: o autor, 2018

TABELA 6 Percentuais de operações diurno e noturno (março 2018)

Operação Noturna	Freq	% op
Pouso	1302	57,3 %
Decolagem	970	42,7 %
Total Op. Noturna	2272	17,1 %
Operação Diurna	**Freq**	**% op**
Pouso	5436	49,5 %
Decolagem	5552	50,5 %
Total Op Diruna	10988	82,9 %
Total Pouso	6738	50,8 %
Total Decolagem	6522	49,2 %
Total Pouso + Decolagem	13260	

Fonte: o autor, 2018.

TABELA 7 Percentuais de operações diurno e noturno por cabeceira (março 2017)

Cabeceira	11 L		11 R		29 L		29 R	
	Diurno	Noturno	Diurno	Noturno	Diurno	Noturno	Diurno	Noturno
Pouso	2292	283	2286	283	680	84	677	84
	38,8 %	41,0 %	38,7 %	37,0 %	11,5 %	11,0 %	11,0 %	11,0 %
Decolagem	1926	238	2787	345	829	102	418	52
	32,3 %	32,4 %	46,8 %	46,9 %	13,9 %	13,7 %	7,0 %	7,0 %
Total	**4218**	**521**	**5074**	**627**	**1509**	**186**	**1096**	**135**

Fonte: o autor, 2018.

TABELA 8 Percentuais de operações diurno e noturno por cabeceira (março 2018)

Cabeceira	11 L		11 R		29 L		29 R	
	Diurno	Noturno	Diurno	Noturno	Diurno	Noturno	Diurno	Noturno
Pouso	1585	500	1937	184	931	492	983	126
	29,2%	38,4%	35,6%	14,1%	17,1%	37,,8%	18,1%	9,7%
Decolagem	1436	108	2196	417	1207	205	713	240
	25,9%	11,1%	39,6%	43,0%	21,7%	21,1%	12,8%	24,7%
Total	**3021**	**608**	**4133**	**601**	**2138**	**697**	**1696**	**366**

Fonte: o autor, 2018.

Desse modo, conforme indicado nas Tabelas 5 e 6 o total de movimentações considerado foi de 13.366 (março 2017) e 13.260 (março 2018) movimentações/mês. A Tabela 9 mostra a composição da frota de aeronaves para 2017 e 2018. Cabe ressaltar, que a frota de aeronaves utilizada foi a mesma nos dois cenários variando somente os percentuais de operação das aeronaves.

TABELA 9 Composição da frota

Equipamento	mar/17	mar/18
	%	%
PA34	1,10%	1,3%
AT72	2,80%	1,4%
C-208	3,20%	1,1%
ERJ-145	4,00%	0,6%
Total	**100%**	**100%**

Equipamento	mar/17	mar/18
	%	%
ERJ-195	6,10%	5,5%
A318	2,20%	2,1%
A319	10,30%	9,7%
A320	33,10%	36,2%
A321	8,30%	9,5%
A332	0,40%	0,3%
B722	0,40%	0,2%
B737	6,00%	5,8%
B738	20,70%	24,8%
B752	1,40%	1,5%
Total	**100%**	**100%**

Fonte: o autor, 2018.

Para a elaboração das curvas de ruído foi adotada a metodologia prevista no Regulamento Brasileiro de Aviação Civil - RBAC 161 (2013) - que recomenda a simulação de 5 (cinco) curvas (65, 70, 75, 80 e 85), na métrica acústica DNL. As rotas de entrada e saída, utilizadas para os dois cenários, estão expressas em cartas do Tipo SID (Standard Departure Chart) e IAC (Instrument Approach Chart). Destaca-se que são as rotas mais recentes em uso no SBBR.

4.3 METODOLOGIA PARA ELABORAÇÃO DOS MAPAS ACÚSTICOS

Não há apontamentos na legislação brasileira de como conduzir, metodologicamente, a elaboração de mapas acústicos. Por isso, nesse estudo será adotada a metodologia indicada pela Agência Portuguesa do Ambiente (APA). A APA segue as recomendações da Diretiva Europeia 2002/49/CE, cujo objetivo é definir uma abordagem comum para evitar, prevenir ou reduzir, numa base prioritária, os efeitos prejudiciais da exposição ao ruído ambiente, incluindo o incômodo dela decorrente. A Tabela 10 mostra os principais pontos a serem observados no método da APA, para a elaboração das curvas de ruído (do ruído aeronáutico), para a confecção dos mapas acústicos.

TABELA 10 Principais pontos metodológicos - APA (2011)

	Indicador acústico*: Por exemplo: L_{den} ou L_n.
Curva de ruído	Caracterização física: Comprimento da(s) pista(s), coordenadas do início e fim da(s) pista(s) e de outros pontos de referência, tais como o landing threshold (a partir do qual a aeronave pode tocar na pista) e o takeoff point (onde a aceleração para a decolagem se inicia), geometria das rotas e perfis de voo (à descolagem e à aterragem)
	Caracterização quantitativa (dados de emissão): tipo específico de aeronave (discriminado ao tipo e número de motor(es), complementado com informação da certificação acústica da aeronave; n.o de movimentos por: tipo específico de aeronave; período de referência (diurno, entardecer, noturno); tipo de operação (aterragem/descolagem); para cada tipo de aeronave: percentagens de utilização de cada pista e rota; categoria do voo à descolagem;
	Dados meteorológicos: Especialmente em condições de campo aberto em áreas extensas, ou com receptores ou fontes sonoras em altura (por exemplo, ruído de tráfego aéreo), a consideração dos efeitos meteorológicos torna-se determinante para a obtenção de resultados rigorosos, pelo que devem ser utilizados, sempre que disponíveis, dados meteorológicos detalhados do local.
	Validação de longa duração: É essencial, de forma a conferir robustez ao mapa de ruído, que se proceda a uma validação dos resultados. Para tal, os valores apresentados no mapa devem ser comparados com valores de medições efetuadas em locais selecionados.
Mapas Acústicos	Peças escritas (memória descritiva e resumo não técnico) e peças desenhadas (cartogramas). Essas peças (mapas) devem estar georeferenciados. A memória descritiva deve conter a explicação das condições em que foi elaborado o mapa e dos pressupostos considerados, incluindo os dados de entrada; o resumo não técnico, destinado à divulgação ao público, deve incluir os cartogramas. Os mapas acústicos devem ter uma escala igual ou superior a 1:25 000

Nota: * No caso do Brasil: DNL. Fonte: o autor, 2018.

A Figura 2 foi utilizada como referência para a elaboração da relação cores/padrões--classes de níveis sonoros dos mapas de ruídos. Para obter uma melhor definição dessas, já que acima de 70 não teria uma diferenciação da cor no mapa, foi adaptado os níveis DNL 80 e 85 com RGB de 29/75/241 e 100/69/40, respectivamente.

FIGURA 2 Relação de cores e padrões para as classes de níveis sonoros.

Classe do Indicador	Cor		RGB
$L_{den} \leq 55$	ocre		255, 217, 0
$55 < L_{den} \leq 60$	laranja		255, 179, 0
$60 < L_{den} \leq 65$	vermelhão		255, 0, 0
$65 < L_{den} \leq 70$	carmim		196, 20, 37
$L_{den} > 70$	magenta		255, 0, 255
$L_n \leq 45$	verde escuro		0, 181, 0
$45 < L_n \leq 50$	amarelo		255, 255, 69
$50 < L_n \leq 55$	ocre		255, 217, 0
$55 < L_n \leq 60$	laranja		255, 179, 0
$L_n > 60$	vermelhão		255, 0, 0

Fonte: APA, 2011.

Para a elaboração dos mapas de ruído foi utilizado o programa de Sistema de Informação Geográfica, QGIS que é um sistema de código aberto. O QGIS é um projeto oficial do Open Source Geospatial Foundation (OSGEO) e suporta inúmeros formatos arquivos vetorizados, arquivos rasters (matriciais) e bases de dados. A versão utilizada foi o QGIS 2.18 onde pode-se visualizar, gerir, editar, criar mapas e analisar dados. Os dados de base utilizados foram:

(A) Dados dos Setores Censitários do DF, em formato shape (shp) e informação para cada subsecção estatística (dados do Censo 2010, IBGE);

(B) Dados das curvas de ruído simuladas no INM 7.0d, em formato shape (shp);

(C) Dados matriciais (Mosaico DF 2009), em formato shape (shp);

(D) Dados de localização e limites do sítio do SBBR, em formato shape (shp);

(E) Dados de Edifícios do DF – Base SICAD 2010.

A Tabela 11 mostra os limites de cada curva de ruído gerada e expressas nos mapas.

TABELA 11 Indicadores acústicos das curvas de ruído

Indicador DNL
DNL 50 = 50 < DNL ≤ 55
DNL 55 = 55 < DNL ≤ 60
DNL 60 = 60 < DNL ≤ 65
DNL 65 = 65 < DNL ≤ 70
DNL 70 = 70 < DNL ≤ 75
DNL 75 = 75 < DNL ≤ 80
DNL 80 = 80 < DNL ≤ 85
DNL 85 = DNL > 85

Fonte: o autor, 2018.

5. RESULTADOS E DISCUSSÃO

Em relação às pistas, a Tabela 12 mostra o percentual de movimentos, por cabeceira, nos dois cenários. Para o cenário 1 tem-se 43% de operação (pousos mais decolagens) na pista 1 e 57% na pista 2. Já para o cenário 2 tem-se 44% de operação na pista 1 e 56% na pista 2. Desse modo, foi observado um percentual maior de utilização da pista 2 (11R/29L) nos dois cenários. Essa pista está mais próxima ao Park Way e a pista 1 (11L/29R) próxima ao Lago Sul. Talvez explique essa concentração na pista 2 um número maior de voos com destino às principais cidades do Sudeste e Sul do país que decolam preferencialmente dessa pista.

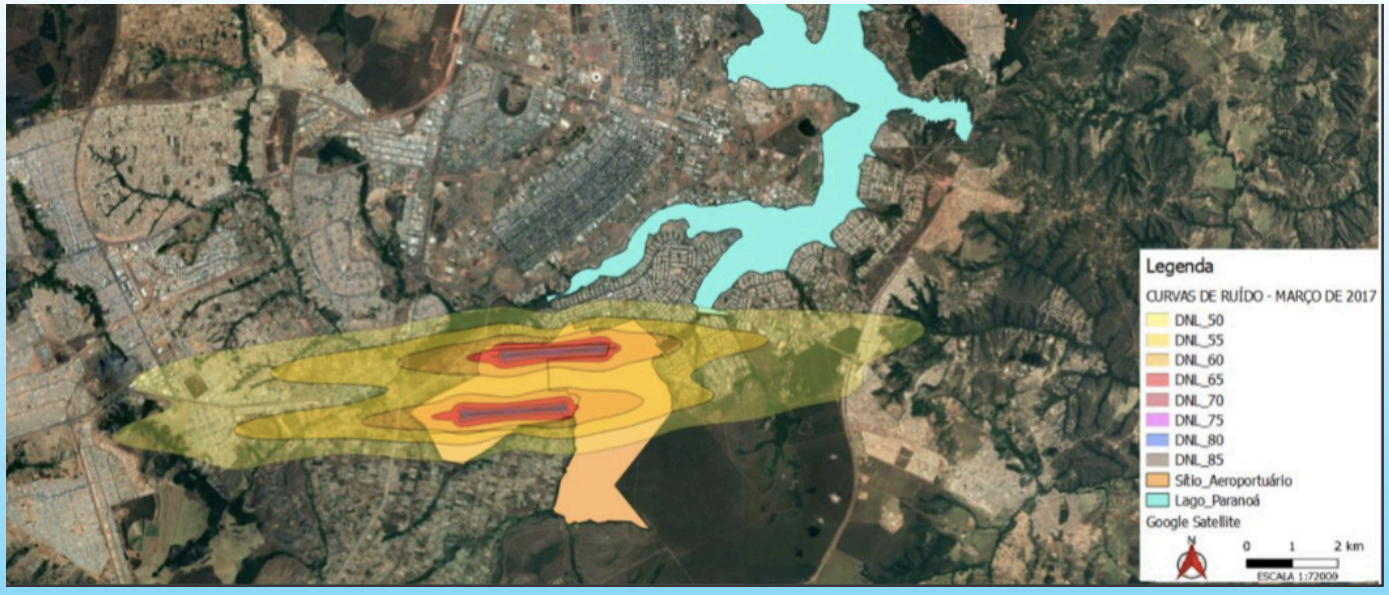
TABELA 12 Total de movimentos por cabeceira 2017 – 2018

Pista	Cabeceira	mar/18		mar/17	
		Total	% Total	Total	% Total
Pista 1	11 L	3629	27 %	4739	35 %
	29 R	2062	16 %	1231	9 %
Pista 2	11 R	4734	36 %	5701	43 %
	29 L	2835	21 %	1695	13 %
Total		13260	100%	13366	100%

Fonte: o autor, 2018.

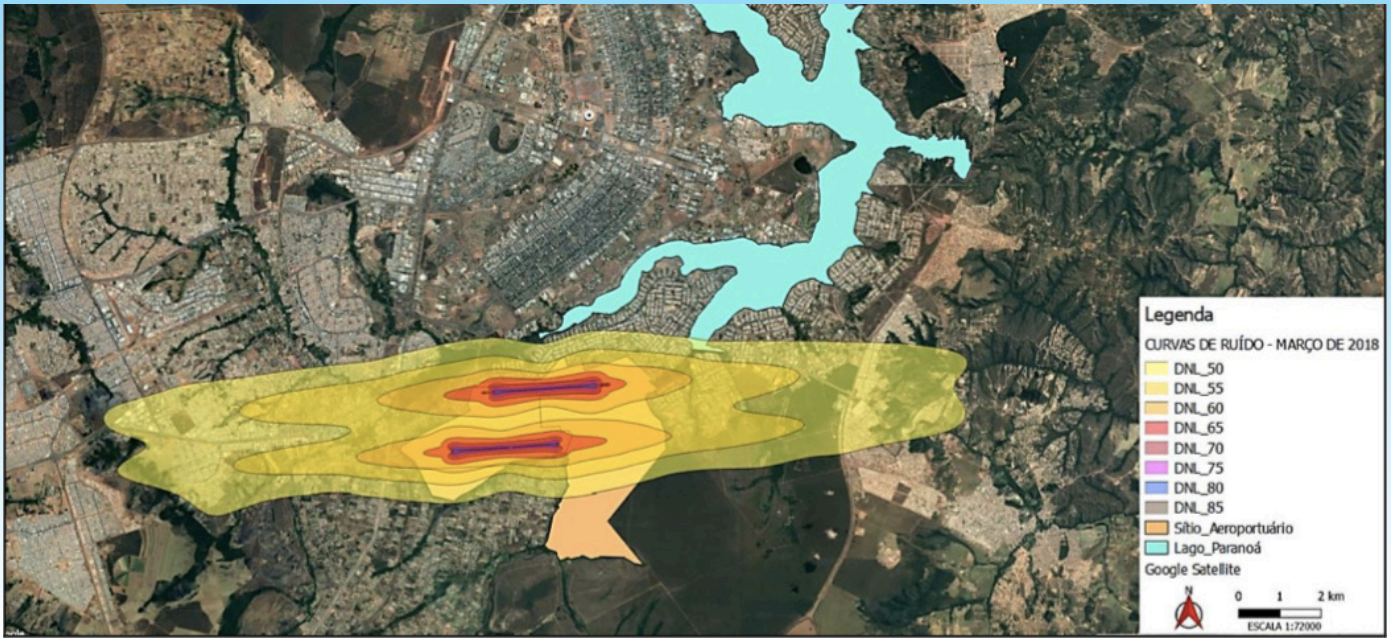
As Figuras 3 e 4 mostram os mapas de ruídos elaborados para os cenários 1 e 2, ou seja, entre o mês de março de 2017 e o mês de março de 2018.

FIGURA 3 Mapa de ruído SBBR - Março 2017



Fonte: o autor, 2018.

FIGURA 4 Mapa de ruído SBBR - Março 2018



Fonte: o autor, 2018.

Nas Figuras 3 e 4 é possível observar as regiões afetadas pelo ruído aeronáutico em ambos os cenários. Cabe ressaltar, que esses são mapas que indicam o impacto sonoro para um mês de operação e não para um ano inteiro. Para os dois cenários, considerando as curvas de ruído DNL 50 e 55, verifica-se que a leste do SBBR essas curvas estendem-se até Taguatinga e Samambaia, devido às operações na pista 1, e até o Riacho Fundo para os movimentos na pista 2. A oeste, essas curvas de ruído, considerando a pista 1, atingem regiões do Lago Sul, Setor de Mansões Dom Bosco e Jardim Botânico. Ao norte da pista 1 as curvas de ruído englobam quadras do Lago Sul e ao sul da pista 2, chegam ao Park Way (quadras 14, 19, 21, 23 e 25).

A leste, as operações na pista 1 fazem com que a curva de ruído DNL 60 chegue no Park Way (quadra 3) atingindo partes do Setor Habitacional Arniqueiras. Para a pista 2, essa curva avança para as quadras 6 e 7 do Park Way e áreas do Núcleo Bandeirante (Vila Metropolitana). A norte da pista 1 a DNL 60 passa pelas quadras 01 e 13 do Lago Sul.

Na parte Sul da pista 2, a DNL 60 chega ao Park Way (quadras 14, 19, 21, 23 e 25)

em partes mais próximas ao limite do sítio aeroportuário. A curva de ruído DNL 65 atinge uma parte do Núcleo Bandeirante, resultante da operação na pista 1 e uma pequena parte do Park Way (quadra 14) devido aos movimentos na pista 2. As demais curvas estão restritas aos limites do sítio aeroportuário não atingindo áreas de uso residencial ou misto.

Comparando os mapas, verifica-se a existência de uma pequena diferença (principalmente nas DNL´s 65 – 85) entre as regiões atingidas pelo ruído, que pode ser melhor observada na Tabela 13 que compara o tamanho das áreas, em km2, de cada curva nos dois cenários. Essa pequena diferença já era esperada, uma vez que a frota simulada foi a mesma para os dois anos e as diferenças percentuais de operações não foram muito significativas nos dois cenários. Além disso, o regime de vento nas cabeceiras muda muito pouco de um ano para outro.

TABELA 13 Comparação entre as áreas 2017 - 2018

DNL	ÁREA (Km²)		
	2017	2018	Diferença
50	95,5	112,7	17,2
55	45,0	54,5	9,5
60	17,4	22,3	4,9
65	5,7	7,5	1,8
70	2,6	3,1	0,5
75	1,2	1,5	0,3
80	0,5	0,6	0,2
85	0,1	0,2	0,1

Fonte: o autor, 2018.

As Figuras de 5 a 8 mostram essa diferença das curvas de ruído em uma comparação entre o mês de março dos anos de 2017 e 2018. Nessas figuras não foram usadas o sistema de cores padronizadas para melhor visualização de comparação.

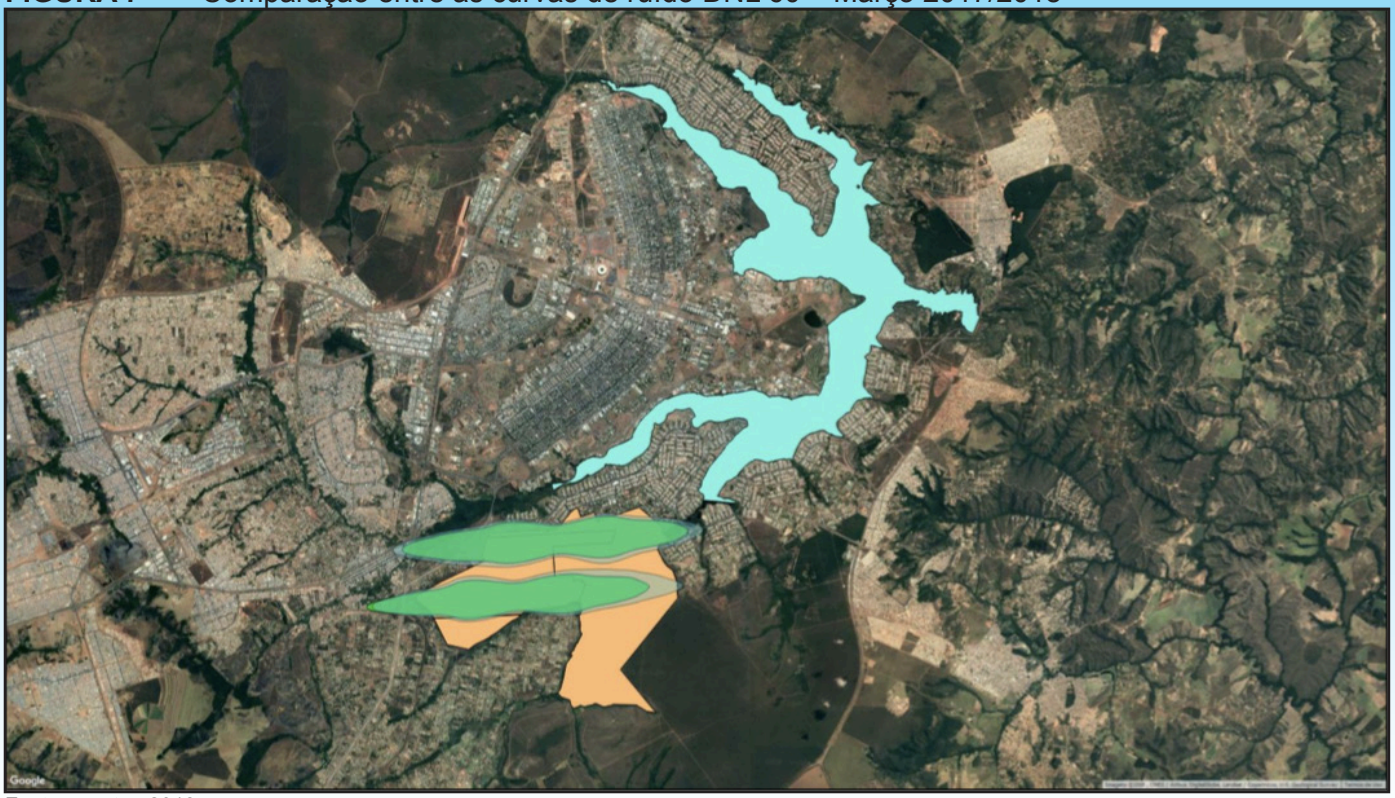
FIGURA 5 Comparação entre as curvas de ruído DNL 50 – Março 2017/2018

Fonte: o autor, 2018.

FIGURA 6 Comparação entre as curvas de ruído DNL 55 – Março 2017/2018

Fonte: o autor, 2018

FIGURA 7 Comparação entre as curvas de ruído DNL 60 – Março 2017/2018



Fonte: o autor, 2018

FIGURA 8 Comparação entre as curvas de ruído DNL 65 – Março 2017/2018

Fonte: o autor, 2018.

Dessa forma, com base na avaliação qualitativa realizada, de comparação entre os tamanhos das curvas de ruído, não se espera mudança expressiva de aumento da população exposta ao ruído aeronáutico no interior dessas curvas. O estudo desenvolvido por Carvalho Jr, E (2015) apresenta os resultados do percentual da população exposta ao ruído aeronáutico, decorrente do SBBR, para cada DNL (com dados de operação dos anos de 2014 e 2015).

A Tabela 14 resume os resultados obtidos por Carvalho Jr, E (2015), destacando para as curvas mais ruidosas:

- DNL 60: As RA's do Núcleo Bandeirante, Park Way e Lago Sul são as com o maior número de pessoas expostas;
- DNL 65: Núcleo Bandeirante se destaca como a região mais afetada com, aproximadamente, 5% da população exposta, seguido por Lago Sul (2,3%) e Park Way (4%).
- DNL 70: 129 pessoas afetadas. Esse número de pessoas é pequeno, mas indica a ocupação de áreas muito próximas aos limites do sítio aeroportuário onde, segundo o RBAC 161 (2013), os projetos das residências deveriam apresentar medidas para se atingir uma redução de ruído de pelo menos 25 dB.

Para a curva DNL 55 as RA's, do Núcleo Bandeirante, Park Way, Candangolândia e Lago Sul apresentam percentual considerável de população exposta. Entretanto, destaca-se nessa DNL a RA do Riacho Fundo com 73% da população exposta. Já na DNL 50 novamente destacam-se com percentual de população significativo o Lago Sul, Candangolândia e Park Way. Além dessas RA's, para Taguatinga (região Sul) também foi obtido um percentual considerável (28%) de população exposta.

TABELA 14 População exposta estimada por curva de ruído DNL

RA	Pop. RA	DNL 50		DNL 55		DNL 60		DNL 65		DNL 70	
		PE	% PE	PE	% PE	PE	% PE	PE	% PE	PE	% PE
Brasília	221.223	1.635	1,0	-	-	-	-	-	-	-	-
Candangolândia	16.799	7.155	43,0	4.603	27,0	1.428	9,0	-	-	-	-
Guará	125.808	8.841	7,0	1.385	1,0	834*	1,0	-	-	-	-
Lago Sul	31.206	9.438	30,0	6.777	22,0	3.946	13,0	714	2,3	89	0,3
Núcleo Bandeirante	23.714	-	-	2.609	11,0	21.180	89,0	1.172	5,0	-	-
Paranoá	45.613	2.442	5,0	-	-	-	-	-	-	-	-
Park Way	19.759	6.173	31,0	4.069	21,0	3.975	20,0	701	4,0	40	0,2
Riacho Fundo	37.278	8.946	24,0	27.039	73,0	1.074	2,9	-	-	-	-
Samambaia	220.806	3.196	1,0	-	-	-	-	-	-	-	-
Taguatinga	214.282	60.529	28,0	25.780	12,0	615**	0,3	-	-	-	-
Total	1.054.465	113.838	11,0	74.681	13,0	33.052	7,0	2.587	3,0	129	0,2

Fonte: Carvalho Jr, E (2015).

Carvalho Jr, E (2015) também resumiu a população total exposta em cada curva de ruído, bem como estimou o número de pessoas que estariam altamente incomodadas (AI) e incomodadas (I) com o ruído aeroviário. Para tanto, utilizou modelos matemáticos próprios desenvolvidos no âmbito de seu estudo. Esses resultados estão expressos na Tabela 15.

TABELA 15 População exposta e número estimado de I e AI

DNL	PE	% PE	AI	I
50	113.838	11	8.652	23.109
55	74.681	13	10.082	22.479
60	33.052	7	7.503	13.915
65	2.587	3	924	1.428
70	129	0,2	66	87

Fonte: Carvalho Jr, E (2015).

Da Tabela 15 observa-se um total de 8.652 indivíduos altamente incomodados (AI) e 23.109 incomodados na DNL 50. Taguatinga destaca-se com o maior número de pessoas afetadas. Na DNL 55 foi estimado um total de 10.082 pessoas altamente incomodadas e 22.479 incomodadas. Na DNL 60, tem-se um total estimado de 7.503 pessoas altamente incomodadas e 13.915 incomodadas. Já na DNL 65 924 indivíduos estariam altamente incomodados e 1.428 incomodados. Na DNL 70 a população exposta é muito pequena, porém indica a ocupação de áreas nos limites do sítio aeroportuário. Esses indivíduos podem desencadear uma série de ações contrárias à operação de aeronaves em algumas rotas e horários. Essas ações podem levar ao desenvolvimento de conflitos, entre a comunidade e o operador do SBBR, devido ao incômodo sonoro induzido pelo ruído aeroviário.

Carvalho Jr, E (2015) ressalta que estimar o percentual de pessoas incomodadas ou altamente incomodadas, colabora para uma melhor compreensão dos impactos causados pelo ruído aeroviário na população exposta. Com essas informações o operador do SBBR, as autoridades públicas e a comunidade local podem trabalhar em estratégias capazes de satisfazer não só a demanda pelo transporte aéreo, mas também viabilizar o desenvolvimento de medidas que minimizem a exposição das comunidades ao ruído das aeronaves.

CONCLUSÕES

Essa pesquisa avaliou o impacto do ruído aeronáutico no entorno do Aeroporto Internacional de Brasília, após a implementação das operações simultâneas nas suas quatro cabeceiras. Foram elaboradas curvas de ruído e mapas acústicos na métrica acústica DNL para o mês de março de 2017 (operação padrão) e mês de março de 2018 (operação si-

multânea). Em seguida, comparou-se impacto sonoro no entorno do SBBR entre esses meses com diferentes tipos de operação.

A alteração da configuração de operação, baseada no cenário 1 para o cenário 2, não resultou em impactos expressivos de ruído aeronáutico nas áreas circunvizinhas ao Aeroporto de Brasília. Todavia, verificou-se uma população exposta significativa ao ruído aeroviário nas DNL's 55 e 60, ou seja, essas curvas atingem regiões de Taguatinga, Samambaia, Riacho Fundo, Setor de Mansões Dom Bosco e Lago Sul.

Essas curvas de ruído ainda estão fora das restrições de uso e ocupação do solo indicados no RBAC 161. Apesar de serem compatíveis com o uso residencial, o ruído aeronáutico nessas regiões é percebido pelos moradores podendo gerar reações. Portanto, as áreas sob essas curvas devem ser incluídas em estudos de impactos ambientais. Cabe ressaltar que a crescente demanda por operações no SBBR e sua proximidade com áreas residenciais apontam para uma situação de comprometimento do ambiente sonoro das áreas circunvizinhas no seu entorno com significativo potencial de incômodo conforme constatou a pesquisa de Carvalho Jr, E (2015).

Sugere-se para estudos futuros a simulação das curvas de ruído para um ano completo de operações simultâneas independentes. A partir dessas simulações elaborar mapas de ruído, estimar a população exposta e quantificar o incômodo sonoro, inclusive no período noturno, nas áreas circunvizinhas ao SBBR.

EVALUATION OF THE IMPACT OF AERONAUTICAL NOISE IN THE BRASILIA ENVIRONMENT

ABSTRACT: The present study evaluated the impact of aeronautical noise, around the International Airport of Brasilia, after the implementation of the simultaneous operations in their four headwaters. It became, the first airport of South America operating with independent headwaters. For that, noise curves were elaborated with data provided by INFRAMERICA. The isophonics were simulated in INM 7.0d software based on the methodology described in the Brazilian Civil Aviation Regulation 161 (2013). The acoustic metric adopted was the DNL (day-night average sound level). A GIS tool was also used for the elaboration of noise maps. Simulations were performed for two scenarios. The first to March 2017, where landing and take-off operations took place in the standard format (with landing movements taking place preferentially on one runway and takeoff operations on another). The second scenario was for March 2018 where only simultaneous operations took place in the four headwaters. The total number of transactions was 13,366 (2017) and 13,260 (2018) movements / month. Based on the generated noise curves, there were no significant changes among the scenarios in relation to aeronautical noise in the areas surrounding the airport. However, there was a significant population exposed to airborne noise in DNL's 55 and 60 (outside the restrictions of land use and occupation indicated in RBAC 161) that reach regions of Taguatinga, Samambaia, Riacho Fundo, Setor de Mansões Don Bosco and Lago Sul. Despite being compatible with the residential use, the aeronautical noise in these regions is perceived by the residents and can generate reactions.

Keyword. Aeronautical noise. Sound Zoning. Noise maps. Environmental impact.

REFERÊNCIAS

ABNT (1990) NBR 11.415: Ruído Aeronáutico. Associação Brasileira de Normas Técnicas, Rio de Janeiro.

ABNT (2000) NBR 10.151 - Avaliação do Ruído em Áreas Habitadas, Visando o Conforto da Comunidade. Associação Brasileira de Normas Técnicas, Rio de Janeiro.

APA (2011) Agência Portuguesa do Ambiente. Directrizes para elaboração de mapas de ruído versão 3. Disponível em:<http://www.apambiente.pt/_zdata/DAR/Ruido/NotasTecnicas_EstudosReferencia/DirectrizesMapasDez2011_todo_2.pdf >. Data de acesso: 18 de março de 2018.

Babisch, W (2002). The Noise/Stress Concept, Risk Assessment and Research Needs. Noise Health, v. 4, n. 16, p.1-11.

Babisch W., Houthuijs D., Pershagen G., Cadum E., Katsouyanni K., Velonakis M., Dudley M.L., Marohn H.D.,Swart W., Breugelmans O., Bluhm G., Selander

J., Vigna-Taglianti F., Pisani S., Haralabidis A., Dimakopoulou K., Zachos I., Jarup L (2009). Annoyance due to aircraft noise has increased over the years-results of the HYENA study. Environment International, v. 35, n. 8, p. 1169 - 1176.

Bonatto, A. S (2013) Caracterização e simulação do ruído aerodinâmico gerado por “slats”. Dissertação mestrado – Escola politécnica da Universidade de São Paulo.Departamento de Engenharia Mecânica. São Paulo. SP.

Brooker, P. (2006) Aircraft Noise: Annoyance, House Prices and Valuation. Acoustics Bulletin, may/june, IOA. P.29-32.

BSBAERO (2013), Aeroporto Internacional de Brasília. Disponível em: http://www.bsb.aero/institucional Data de acesso: 12 de julho de 2018.

Carvalho Júnior, E. B.; Garavelli, S. L.; Maroja, A. M (2012) Analysis of the effects of aircraft noise in residential areas surrounding the Brasilia International Airport. Journal of Transport Literature; v. 6, n. 4, p. 59 – 81.

Carvalho Jr, E. B., Garavelli, S. L., Smozinski, F. V., Maroja, A. M. e Melo, W. C. (2013) Análise das principais métricas utilizadas no zoneamento acústico de áreas próximas a aeródromos. Journal of Transport Literature, vol. 7, n. 4, p. 175 - 198.

Carvalho Júnior, E. B.; Garavelli, S. L., Barros, A. G., Araújo, R. B., Maroja, A. M e Shimoishi, J. M (2014a) Análise do efeito do ruído aeronáutico sobre o preço de imóveis residenciais: estudo de caso do Aeroporto Internacional de Brasília. XXV Encontro da Sociedade Brasileira de Acústica – SOBRAC. Campinas - SP. v.01.

Carvalho Júnior, E. B., Garavelli, S. L., Barros, A. G., Maroja, A. M., Melo, W. C e Shimoishi, J. M (2014b) Ruído Aeronáutico: Análise Comparativa das Metodologias Adotadas no Brasil e na Comunidade Europeia. 6oPLURIS - Congresso Luso- Brasileiro para o Planejamento Urbano, Regional Integrado e Sustentável.Lisboa. Livro de Actas, 2014. v. 01. p. 69 – 80.

Carvalho Júnior, E. B. Quantificação do incômodo gerado pelo ruído aeronáutico por meio de modelos dose-resposta(2015). Tese de Doutorado. Tese de Doutorado– Universidade de Brasília. Faculdade de Tecnologia. Departamento de Engenharia Civil e Ambiental.

Clark, C e Stansfeld, S. A (2011) The Effect of Nocturnal Aircraft Noise on Health : a Review of Recent Evidence. Report prepared for the London Borough of Hounslow. London.

De Barros A. G (2013) Sustainable integration of airports into urban planning – a review, International. Journal ofUrban Sciences, v.17, n. 2, p. 226 – 238.

Dekkers, J.E.C. e Straaten, J.W. (2009). Monetary valuation of aircraft noise: a hedonic analysis around Amsterdamairport. Ecological Economics. v. 68, p. 2850 – 2858.

FAA (2011) Noise and its Effect on People. Federal Aviation Administration. Disponível em:<http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/envir_programs/mase/media/ApxH_NoiseAndItsEffectOnPeople_122805.pdf>. Data de acesso em: 14 novembro de 2017.

Faburel, G. (2005). Properties value depreciation, social segretion and environmental injustice caused by aircraftnoise. The 2005. Congress and Exposition on Noise Control Engineering. Rio de Janeiro - Brazil: Inter-noise.

Feitelson, E.I., Hurd, R.E. e Mudge R.R. (1996) The impact of airport noise on willingness to pay for residences,Transportation Research Part D, v. 1, p. 1–14.

FICAN (1997) Federal Interagency Committe on Aviation Noise - Effects of Aviation Noise on Awakenings from Sleep. Disponível em: <http://www.fican.org/pdf/Effects_AviationNoise_Sleep.pdf Data de acesso: 10 de dezembro de 2017.>

Girvin. R (2009) Aircraft noise-abatement and mitigation strategies. Journal of Air Transport Management, v. 15,p. 14 – 22.

GUEDES, Margarida; LEITE, Maria João; SEQUEIRA, Nuno. Directrizes para elaboração de mapas de ruído. Agência Portuguesa do Ambiente, 2011.

Haralabidis A. S., Dimakopoulou K, Vigna-Taglianti F, Giampaolo M, Borgini A, Dudley ML, Pershagen G, Bluhm G, Houthuijs D, Babisch W, VelonakisM,Katsouyanni K, Jarup L (2008). Acute effects of night-time noise exposure on blood pressure in populations living near airports. European Heart Journal, v. 29, n. 5, 658-64.

Heleno, T. A (2010) Uma nova metodologia de zoneamento aeroportuário com o objetivo de reduzir o encroachment e os efeitos adversos do ruído. Dissertação de mestrado. Universidade Federal do Rio de Janeiro (UFRJ).

IAC 4102 (1981) Métodos de avaliação dos níveis de ruído e de incômodo gerados pela operação de aeronaves emaeroportos. Intituto de Aviação Civil. Ministério da Aeronáutica. Rio de Janeiro.

ICAO (2002) Airport Planning Manual, Part 2, Land Use and Environmental Protection – Doc 1984. International Civil Aviation Organization.

Jarup L., Dudley ML., Babisch W., Houthuijs D., Swart W., Pershagen G., Bluhm G., Katsouyanni K., Velonakis M., Cadum E. e Vigna-Taglianti F (2005) Hypertension and Exposure to Noise near Airports (HYENA):Study Design and Noise Exposure Assessment. Environmental Health Perspectives. n. 113, p. 1473-1478.

Jones, K (2009). Aircraft Noise and Sleep Disturbance: A Review. Environmental Research and Consultancy Department (ERCD). UK. Report 0905. England.

Kroesen, M., Molin E.J.E., Miedema H.M.E., Vos H., Janssen S.A e Wee B (2010) Estimation of the effects ofaircraft noise on residential satisfaction. Transportation Research Part D. v. 15, 144 – 153.

Matos, J.C.B., Flindell, I., Masurier,P e Pownall, C (2013) A comparison of hedonic price and stated preference methods to derive monetary values for aircraft noise disturbance and annoyance. Transportation Research Part D. v. 20, p. 40 – 47.

Morrell P e Lu C.H. –Y (2000) Aircraft noise social cost and charge mechanisms – a case study of Amsterdam Airport Schiphol. Transport Research Part D. v. 5, n. 4, p.305–20.

Navrud, S (2002) The State-Of-The-Art on Economic Valuation of Noise. Final Report to European Comission DGEnvironment, Department of Economics and Social Sciences. Agricultural University of Norway.

Nelson, J. P (2004) Meta-Analysis of Airport Noise and Hedonic Property Values: Problems and Prospects. Journal of Transport Economics and Policy, v. 38, n. 1, p. 1- 28.

Püschel, R e Evangelinos, C (2012) Evaluating noise annoyance cost recovery at Düsseldorf International Airport.Transportation Research Part D. v. 17, n. 8, p. 598– 604.

RBAC (2013) Regulamento Brasileiro da Aviação Civil (161). Planos de Zoneamento de Ruído de Aeródromos. Aprovado na resolução n. 281, de 10 de setembro de 2013, publicado no Diário Oficial da União de 13 desetembro de 2013, Seção 1, p. 14 – 15.

Rocha, R. e Slama, J (2008) Adequação do zoneamento urbano ao zoneamento sonoro dos aeroportos. VII SITRAER,p. 629-640 – Tr. 512.

SadrMK.,NassiriP,HosseiniM,MonavariMeGharagozlou A (2014) Assessment of land use compatibility and noise pollution at Imam Khomeini International Airport. Journal of Air Transport Management, v. 34, p. 49 – 56.

Suau-Sanchez P, Pallares-Barbera, M e Paül V (2011). Incorporating annoyance in airport environmental policy: noise, societal response and community participation. Journal of Transport Geography. v.19, p. 275 –284.

WHO (2009) World Health Organization. Night noise guidelines for europe. W.H.O Regional Office for Europe. Copenhagen.

Patrícia dos Reis de Morais é graduada em Engenharia Civil. Possui cursos na área de QiBuilder elétrico, hidrossanitário, AutoCAD e QGIS 2.18. Atualmente, exerce a função de estagiário na empresa Ecta Engenharia e pode ser contactada pelo email patricia.reis@sempreceub.com.

Raphaella de Souza Serapião Amorim, é graduada em Engenharia Civil. Possui cursos na área de Revit, Eberick, Mcalc 3D, QGIS 2.18, QiBuilder elétrico, hidrossanitário, AutoCAD. Atualmente, exerce a função de estagiário na empresa Ecta Engenharia na elaboração de projetos Estruturais de aço, concreto armado, fundação, laudo de inspeção predial e laudo de sondagem e pode ser contactada pelo email raphaella.amorim@sempreceub.com.

O orientador, Edson Benício de Carvalho Júnior, é pesquisador e professor nos cursos de Engenharia Civil da Universidade Católica de Brasília (UCB) e do Centro Universitário de Brasília (UniCEUB). Trabalho com os seguintes temas: Transporte e Meio Ambiente; Monitoramento e controle de poluentes atmosféricos de fontes de transportes; Vibração; Simulação em Acústica Ambiental (elaboração de mapas acústicos); Desenvolvimento de Planos de Zoneamento de Ruído (PZR e PEZR) para Aeroportos; Monitoramento e Controle de Ruído Ambiente; Ruído Ambiente e Relações Dose-resposta. Entre 2013 e 2014 cursei doutorado sanduíche na Universidade de Calgary - Canadá.

CICAD.II.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

IMPLEMENTAÇÃO DE TESTES DE INVASÃO EM APOIO À PROTEÇÃO CIBERNÉTICA DE REDES E SISTEMAS DE INTERESSE DA DEFESA

Luiz Henrique Filadelfo Cardoso[1], Lucas Maurício Alves Zigunow[2]

Pós-graduado em Gestão de Segurança da Informação[1], Mestrando em Gestão dos Sistemas de Informação e das Redes[2]

RESUMO: Este trabalho tem como principal objetivo apresentar aspectos fundamentais sobre Testes de Invasão e sobre a sua implementação em apoio à proteção cibernética de redes e sistemas de interesse da Defesa. Buscou-se neste artigo apresentar o atual cenário de proteção, dominado por técnicas e ferramentas de caráter passivo, assim como defender que o apoio da segurança ofensiva, em específico do processo de pentesting, pode ser relevante para o estabelecimento de uma consciência situacional mais equilibrada sobre os ativos de Defesa que se deseja proteger. Para isso, realizou-se uma pesquisa bibliográfica em busca de conceitos consistentes sobre Teste de Invasão, principais modalidades, metodologias aplicáveis e de características que o afastem em entendimento de outras modalidades de avaliações de segurança como Auditoria de Segurança e Análise de Vulnerabilidades. Na sequência, discorreu-se sobre a dinâmica presente nos Testes de Invasão, identificando procedimentos e correlações entre cada fase interdependente e como cada estágio influencia no resultado final de tais testes. Por fim, foram feitas considerações a respeito da implementação do pentesting no contexto militar, apontando caminhos de caráter estrutural, de treinamento e formação de equipes para que os benefícios advindos da adoção de tal prática não se restrinjam apenas a complementar a proteção dos ativos de Defesa, como inicialmente proposto, mas que vá além e contribua também de maneira relevante para formação e adestramento do combatente cibernético brasileiro.

Palavras-chave: Teste de invasão. Segurança ofensiva. Proteção cibernética. Defesa cibernética. Defesa nacional.

INTRODUÇÃO

Em um mundo cada vez mais complexo e interconectado, proteger-se contra a exploração de vulnerabilidades por elaboradas ameaças consiste em diferencial de grande valia para Estados e organizações que desejam permanecer ativos e operacionais, principalmente a partir do ciberespaço.

Nesse contexto, o uso de métodos, técnicas, ferramentas e procedimentos adequados de segurança, aliado ao pleno entendimento sobre eventuais vulnerabilidades identificadas (e do potencial impacto caso sejam exploradas), é competência que os responsáveis pela proteção cibernética de sistemas e redes de interesse da Defesa Nacional devem se valer durante 24 horas por dia, 7 dias por semana.

Porém, ainda que estes profissionais sigam políticas, melhores práticas e recomendações de segurança, assim como monitorem a infraestrutura sob sua responsabilidade de maneira ininterrupta, tradicionalmente não há a presença do olhar ofensivo, com viés do invasor, na detecção de vulnerabilidades, o que efetivamente traria uma consciência situacional mais adequada do ambiente a ser protegido. Ou seja, há a primazia da ótica defensiva com ênfase na reação (ação após incidentes e configuração de soluções de caráter passivo), em detrimento de uma visão expandida na qual também teria espaço a mimetização do mindset proativo do hacker na percepção de ameaças e proposição de medidas de segurança customizadas. A fim de reduzir essa lacuna e cumprir a máxima de que “Para pegar o invasor, deve-se pensar igual a ele”, emerge como disciplina complementar a Segurança Ofensiva.

Segurança Ofensiva pode ser definida como o conjunto de ações proativas que visa

descobrir brechas de segurança, por meio da aplicação de técnicas e ferramentas usualmente utilizadas por criminosos cibernéticos, com o intuito de analisar a extensão e impacto de eventuais ataques antes que vulnerabilidades sejam exploradas pelos referidos atores ou outros agentes adversos. Posto isto, o processo baseado em metodologia específica e técnicas avançadas que melhor se coaduna ao atendimento dos objetivos supramencionados é o Teste de Invasão.

Importante ainda expor que, para esse trabalho, o entendimento de redes e sistemas de interesse da Defesa correlaciona-se às infraestruturas de Tecnologia da Informação e Comunicação (TIC), inclusive infraestruturas críticas, que sejam essenciais para os interesses do Ministério da Defesa, cumprimento da missão das Forças Singulares e para a continuidade da sociedade da informação, conforme depreendido de Brasil (2014).

Sendo assim, este artigo foi organizado da seguinte forma: Seção I apresenta definição de Teste de Invasão, principais tipos, metodologias aplicáveis e sua distinção em relação a outras modalidades de avaliações de segurança como auditoria de segurança e análise de vulnerabilidades; na Seção II serão detalhadas as fases presentes em um Teste de Invasão, com base no recomendado pela metodologia PTES; já na Seção III discorre-se sobre a implementação do Teste de Invasão no contexto militar; e por fim são tecidas as conclusões sobre o estudo realizado.

1 TESTE DE INVASÃO

Em consonância ao apresentado por Weidman (2014, p.30), Teste de Invasão (ou Pentesting) pode ser interpretado como uma simulação de ataques reais destinada a avaliar os riscos e impactos associados a brechas de seguranças identificadas (caso sejam exploradas). A referida autora também acrescenta que diferente de auditoria de segurança e de análise de vulnerabilidades, onde aquela visa checar o cumprimento de controles previamente definidos e esta a identificar e analisar vulnerabilidades sem necessariamente explorá-las, a finalidade de um teste de invasão vai além ao utilizar métodos e técnicas de um atacante para não somente identificar brechas de segurança, mas para também analisá-las profundamente, explorando-as quando viável, a fim de avaliar o que pretensos invasores poderiam obter após uma exploração bem sucedida das vulnerabilidades encontradas.

Em uma outra definição, esta advinda da empresa de segurança Ec-Council extraída de seu curso Certified Ethical Hacker V.9, depreende-se que:

> Teste de invasão é um método de avaliação de segurança voltado a um sistema de informação ou rede por meio da simulação de um ataque para encontrar vulnerabilidades que atacantes poderiam explorar; [e que] um teste de invasão não apenas descobre vulnerabilidades, mas também documenta como elas podem ser exploradas (CEH, 2017, mod.1, p.59).

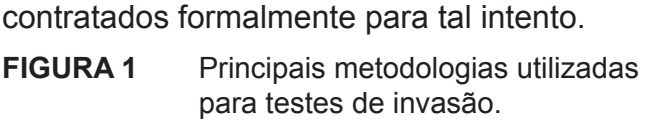
Testes de invasão são ainda subdivididos em três tipos básicos em relação ao conhecimento sobre da infraestrutura a ser testada, quais sejam: black-box - quando não há conhecimento prévio da infraestrutura a ser testada; gray-box - conhecimento parcial da infraestrutura que necessita ser testada; e white-box - quando há total conhecimento sobre a infraestrutura objeto de testes (CEH, 2017).

É importante destacar que o escopo do pentesting não se restringe apenas a testes na esfera lógica de redes e sistemas, mas também o foco da verificação pode ser estendido para testar controles físicos de acesso e avaliação do nível de conscientização de segurança dos colaboradores de uma organização. Alguns especialistas defendem ainda uma outra subdivisão voltada a origem do teste de invasão em: teste de invasão externo - no qual os ataques simulados partiriam de “fora para dentro” da organização, por exemplo via Internet e (ou) via engenharia social; e teste de invasão interno - no qual, por exemplo, simular-se-ia um colaborador descontente com intenções maliciosas

dentro da organização com acesso a sistemas, redes, salas, documentos etc, objetivando-se verificar o grau de segurança de tais ativos e as eventuais consequências danosas caso se confirme o cenário testado (WEIDMAN, 2014).

Por demandar um caráter multidisciplinar dos profissionais que realizam tais testes (pentester), é mandatório que eles sejam organizados em equipes formadas de acordo com os conhecimentos requeridos no escopo do teste (forense computacional, desenvolvimento web, análise de malwares, criptografia, redes Wi-Fi, administração de redes e servidores etc). Uma outra questão reside no vínculo dos integrantes das equipes de pentesting com a organização a ser testada, pois não há a obrigatoriedade de que os pentesters pertençam exclusivamente ao quadro de colaboradores da organização (ainda que seja oportuno), desta forma é plausível também que profissionais externos a organização procedam tais ações, devendo tão somente estarem autorizados ou contratados formalmente para tal intento.

FIGURA 1 Principais metodologias utilizadas para testes de invasão.



Fonte: OPTRASECURITY, 2018.

No que tange as principais metodologias empregadas na estruturação de um teste de invasão, destacam-se, conforme apresentado na Figura 1: Penetration Testing Execution Standard (PTES), Open Source Security Testing Methodology Manual (OSSTMM), OWASP Testing Guide e National Institute of Standards and Technology (NIST) guidelines. Dentre as listadas acima, apenas a metodologia PTES foi desenvolvida com o intuito específico de servir como modelo para conformação de testes de invasão. Enquanto a OWASP possui um escopo dedicado a testes em serviços e aplicações web, NIST e OSSTMM possuem escopo mais amplo e voltado a testes de segurança em geral, ainda que customizáveis para a configuração de um pentesting (BERTOGLIO; ZORZO, 2015).

2 FASES DE UM TESTE DE INVASÃO

Com o firme entendimento do que vem a ser Teste de Invasão, torna-se necessário conhecer e entender a sua dinâmica, desde o esboço até a entrega dos resultados ao solicitante do referido teste. A seguir, serão detalhadas as fases presentes em um teste de invasão, com base no recomendado pela metodologia PTES, as quais se resumem em: preparação, coleta de informações, análise de vulnerabilidades, exploração de falhas, pós-exploração de falhas e geração de relatórios.

2.1 PREPARAÇÃO

Antes do início do teste de invasão, os pentesters devem interagir com o solicitante (Cliente) do teste em busca de definir claramente os objetivos e as eventuais restrições para sua realização. Neste momento determina-se, tal qual recomendado por Weidman (2014):

a) escopo do teste: nesta etapa defini-se a extensão e parâmetros do teste, as redes, sistemas e ativos que serão testados, assim como detalham-se quais ações serão realizadas em sistemas que sejam críticos para o negócio da organização, a fim de evitar indisponibilidades. Por exemplo, nesta etapa deve-se fazer algumas das seguintes perguntas: quais sistemas ou faixa de endereços IP serão testados? Será permitido engenharia social nos colaboradores? O solicitante autoriza o uso de exploit ou de uma simples varredura (scan) em seus sistemas críticos?

b) janela de testes: estipula-se, com base no negócio da organização e devidamente acordado com o solicitante, a duração estimada e o horário em que será procedido os testes para que não ocorram descontinuidades em processos importantes de negócio. Por exemplo, sistemas de

email ou web corporativos apenas serem testados fora do horário comercial.

c) contato de responsável da organização para coordenação: é importante definir uma contraparte na organização a ser testada, geralmente o gestor de mais alto nível de TIC, a fim de que o chefe da equipe de pentesters possa contatá-lo caso a equipe faça uma descoberta grave ou outra coordenação relevante durante a realização do teste de invasão.

d) autorização formal para execução do teste: após reuniões entre as partes, nas quais são definidos limites, objetivos, responsabilidades e acordos de confidencialidade, assim como o escopo dos sistemas, redes e processos a serem testados, o produto final de como será conformado o teste de invasão será resumido a um contrato. Este instrumento não é só imprescindível para a organização solicitante resguardar o seu negócio, mas sobretudo é a permissão formal e o passe "fora da prisão" da equipe de pentesters para executar ações invasivas em ativos alheios, ainda que sob teste.

2.2 COLETA DE INFORMAÇÕES

Nesta fase, conforme exposto por Weidman (2014, p. 31), "o pentester procura informações disponíveis sobre o cliente e identifica maneiras em potencial de conectar-se com seus sistemas". Tal coleta pode ocorrer por meio de fontes cibernéticas, humanas ou aberta. Por exemplo, coleta em redes sociais online e websites da organização e de seus funcionários, uso de scanners de porta a fim de identificar serviços, versões e portas abertas em sistemas-alvo e faixas IP de interesse (tal qual exposto abaixo na Figura 2), coleta e análise do lixo da organização, observação da rotina laboral e comportamental de colaboradores de interesse.

FIGURA 2 Resultado de um scanner (Nmap) para descobrir portas, versões e serviços ativos em sistema-alvo.

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-01 11:19 IDT
Nmap scan report for Scanme.Nmap.Org (64.13.134.52)
Host is up (0.18s latency).
rDNS record for 64.13.134.52: scanme.nmap.org
Not shown: 993 filtered ports
PORT      STATE  SERVICE
25/tcp    closed smtp
53/tcp    open   domain
70/tcp    closed gopher
80/tcp    open   http
113/tcp   closed auth
8009/tcp  open   ajp13
31337/tcp closed Elite
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.26
```

Fonte: Tosch, 2011.

É importante que a fase de coleta de informações seja a mais extensa e metódica possível, uma vez que "os achados" serão determinantes para formulação do melhor caminho para acessar os ativos em teste, conforme será visto a seguir, principalmente na fase de modelagem de ameaças.

2.3 MODELAGEM DE AMEAÇAS

De acordo com os dados e informações colhidos na fase anterior em relação aos ativos, sistemas e redes a serem testados, o pentester irá definir um adequado plano de ataque, com base em procedimentos, ferramentas e métodos específicos para o ativo a ser testado. Ou seja, com base no conhecimento obtido serão definidas estratégias para explorar os sistemas, redes e controles sob teste. Nessa fase também é usual a priorização de cada descoberta por ordem de severidade com base no risco de exploração e o seu eventual impacto danoso (ELEARNSECURITY, 2015).

2.4 ANÁLISE DE VULNERABILIDADES

Após os pentesters colherem informações (serviços e versões de sistemas, faixa de endereços IP de interesse, informações sobre hierarquia, colaboradores e setores-chave da organização etc.) e definirem caminhos e estratégias, priorizando quais ações são mais relevantes, chega o momento de descobrir ativamente as vulnerabilidades existentes com a finalidade de se determinar até que ponto suas

estratégias de exploração poderão ser bem-sucedidas (WEIDMAN, 2014).

Nessa fase, os profissionais fazem tentativas para encontrar brechas de segurança nos controles, sistemas, redes e ativos, no intuito de caracterizá-los como vulneráveis, e por consequência, passíveis de serem explorados. A título de exemplo, executar scanners de vulnerabilidades como SqlMap, Nessus, Nikto, OpenVas ou identificar sistemas, serviços, aplicações carentes de atualizações de segurança são algumas das ações realizadas na fase de análise de vulnerabilidades. Um procedimento comum também nessa fase é a consulta ao banco de vulnerabilidades CVE (Common Vulnerabilities and Exposures), o qual concentra a descrição das principais vulnerabilidades identificadas, com a finalidade de, ao se comparar com as versões de serviços ou aplicações testadas, verificar a existência de códigos (exploits), softwares, técnicas ou procedimentos capazes de explorar os ativos sob análise (ROHR, 2017).

2.5 EXPLORAÇÃO DE FALHAS

Para a grande maioria, essa é a fase mais divertida e interessante em um teste de invasão (WEIDMAN, 2014). No entanto, ela apenas será efetiva se as fases anteriores foram realizadas com detalhamento e produziram dados ou inoformações de valor.

Assim, já com as vulnerabilidades encontradas, listadas e analisadas, o próximo passo é ganhar acesso (de preferência com privilégios de administrador) nos ativos sob teste, sempre objetivando não ser detectado e sem deixar rastros.

O uso de email malicioso (phishing), injeção e manipulação de código SQL malicioso, malwares, credenciais padrão, técnicas de engenharia social e exploração por exploits são os vetores mais comuns de exploração de sistemas, a variar apenas sua escolha, de acordo com o perfil do sistema e usuário almejados (CARDOSO, 2017). Uma plataforma comumente utilizada para dar suporte a este intento é o framework Metasploit, nativo da distribuição Kali Linux, voltada especificamente para segurança ofensiva.

2.6 PÓS-EXPLORAÇÃO DE FALHAS

Com acesso ao sistema ou ativo de interesse, na fase de pós-exploração de falhas, são realizados levantamentos a fim de se aferir o que é possível realizar ou extrair com o acesso conquistado ao sistema.

Elevação de privilégios, instalação de códigos maliciosos para manutenção de acesso, possibilidade de movimento lateral para outras máquinas na mesma rede (ou para outras redes), limpeza de rastro e alteração de logs, busca por arquivos e informações sensíveis, extração de credenciais que possam dar acesso a outros ativos são algumas das ações que os pentesters devem tentar nessa fase para compor o relatório final. Essas ações proporcionarão mensurar o eventual impacto caso um agente adverso venha a ter acesso ao ativo sob teste.

2.7 GERAÇÃO DE RELATÓRIOS

Por fim, na fase de geração de relatórios, os pentesters compilam em documento formal as descobertas tanto para os profissionais executivos (alta direção) quanto para o corpo técnico (responsáveis na “linha de frente” pela gestão e manutenção dos ativos sob análise) da organização. Conforme depreende-se de eLearnSecurity (2015, p.6), “o mais importante ao se confeccionar relatórios é evitar fazer uso de jargões ou termos que possam prejudicar a inteligibilidade por parte do público-alvo”.

Esse documento contemplará, ordenadamente e por seções, a dinâmica do teste de invasão realizado: escopo do teste, apontamentos sobre o que é feito de correto, o que está incorreto e pode ser melhorado, vulnerabilidades encontradas, como o acesso foi conseguido, o que foi descoberto, o risco e impacto para o negócio e como corrigir os problemas encontrados (WEIDMAN, 2014, p. 35). Desta forma, se todos os dados e informações foram

colhidos e organizados adequadamente durante o teste, escrever o relatório mostra-se como uma tarefa meramente de síntese em relação às descobertas e recomendações aplicáveis para corrigir as vulnerabilidades identificadas.

Ainda cabe destacar que o recomendável é que a equipe envolvida no teste proceda, com base no relatório final, uma apresentação oral na organização testada com a presença do corpo técnico e de representantes da alta direção, a fim de que para os técnicos sejam elucidadas eventuais dúvidas e para a direção seja salientada a necessidade de resolução das vulnerabilidades encontradas e a importância de suporte à equipe de técnicos para o êxito da correção. Esta exposição deve ser pautada por maturidade e objetividade (e não como um "caça as bruxas" e busca por culpados) tanto por parte do interlocutor, quanto pelos ouvintes (ELEARNSECURITY, 2015).

3 CONSIDERAÇÕES SOBRE A IMPLEMENTAÇÃO DE TESTES DE INVASÃO NO CONTEXTO MILITAR

Ainda que no cenário empresarial a busca por profissionais e a realização de testes de invasão cada vez seja mais requerida, sobretudo em organizações que possuem dados sensíveis e são obrigadas por força de Lei ou por Estatutos a dar respostas a seus sócios, acionistas, mercado e clientes quanto ao grau de segurança cibernética do seu negócio, no contexto militar ainda não é a realidade e instrumento usual tal prática de sergurança (SERPRO, 2018).

De acordo com a Estratégia Nacional de Defesa (BRASIL, 2008), que definiu o desenvolvimento do setor cibernético sob responsabilidade do Exército Brasileiro, o que demandou entre outras ações a criação do Centro de Defesa Cibernética (CDCiber) em 2012 como órgão operacional e o Comando de Defesa Cibernética (ComDCiber) em 2014 como órgão coordenador e gestor da atividade em âmbito nacional, a tarefa de se realizar testes de invasão em redes e sistemas de interesse da Defesa pertenceria - sob autorização e supervisão normativa do ComDCiber - naturalmente ao braço operacional, qual seja o CDCiber.

Porém, devido à restrição quantitativa de pessoal para o escopo amplo e complexo

de testes que se apresenta: universo normativo e tecnológico heterogêneo, unidades militares distribuídas geograficamente, entre o próprio Exército Brasileiro, Marinha do Brasil e o Comando da Aeronáutica; uma proposta alternativa seria transferir parte dessa responsabilidade executiva de realização de testes de invasão, de maneira similar ao que já ocorre com a proteção cibernética nos moldes atuais para cada Força Armada.

Nesse cenário, ficaria a cargo do CD-Ciber: a execução de testes de invasão nas redes e sistemas de interesse do Ministério da Defesa (eventualmente em outros órgãos da Administração Pública Federal e nas forças militares singulares), a preparação de pessoal dedicado para ações de Estado no tocante à Defesa Cibernética e treinamento do pessoal militar (equipes de pentesting) do Exército, Marinha e Aeronáutica para execução de tais testes (por meio da Escola Nacional de Defesa Cibernética - ENaDCiber), respectivamente, no âmbito de cada Força. O ComDCiber seria o órgão responsável por emitir normas basilares (e outras diretivas) sobre a realização de testes de invasão no âmbito da Defesa, sobre a forma e a dinâmica de solicitação e responsabilidades, padronização, desenvolvimento, doutrina, entrega de relatórios e apresentação dos resultados após os testes realizados. Desta forma, cada Força Armada recepcionaria em seu âmbito os pedidos internos de pentesting, assim como definiria o processo de como devem ser executados tais testes em suas redes e sistemas, tornando-os efetivamente um instrumento complementar para prover a proteção cibernética desejada aos ativos sob sua responsabilidade, de maneira oportuna, tempestiva e especializada ao seu contexto e realidade particular.

Outro aspecto que deve ser levado em conta é o treinamento e a estruturação das equipes de pentesting. Diferente do contexto civil em que as equipes são formadas com primazia pela aptidão e especialização de seus integrantes e pouco pelo tempo “de casa” ou hierarquia funcional; no meio militar a estruturação das equipes pode vir a sofrer influência em maior grau pela hierarquia do que pela especialização e aptidão do pentester.

Uma solução equilibrada pode ser considerar tanto na escolha da trilha de formação quanto na estruturação das equipes, o viés

da aptidão, habilidade reconhecida e da experiência anterior, fazendo uso da hierarquia funcional apenas para a posição de gerência ou coordenador de equipe. Por exemplo, em uma equipe formada por três integrantes, o de maior precedência ficaria responsável por coordenar os trabalhos e organização e formalizaçao dos resultados do teste de invasão, os outros dois por sua execução (caso necessário, também com apoio do integrante de maior precedência). Importante ainda acrescentar que a participação regular em exercícios cibernéticos simulados (red team vs blue team), cursos, treinamentos na área, desafios na modalidade CTF (Capture the Flag) e outros eventos nos quais sejam simulados ambientes e situações encontradas também em testes de invasão, contribuem de maneira determinante para a identificação de afinidades e habilidades aproveitáveis no pessoal a ser escolhido para a composição de equipes de pentesting, assim como para o seu devido adestramento e preparo contínuo (LOSPINOSO, 2018).

CONCLUSÕES

Por crer no aforismo de Sun Tzu, o chefe militar mais conhecido da antiguidade, quando este afirma que "conhecer o modo de agir de um oponente é fator preponderante para a vitória", este trabalho buscou apresentar a modalidade teste de invasão, que visa mimetizar métodos, técnicas e ferramentas usadas por criminosos cibernéticos, não para obter vantagens ilícitas, mas sim para complementar a proteção de redes, sistemas e outros ativos de interesse da Defesa.

O artigo definiu o que vem a ser testes de invasão, sua distinção em relação a auditoria de segurança e análise de vulnerabilidades, suas principais abordagens e características.

Também foi exposta a dinâmica presente nas fases de um teste de invasão desde o seu esboço até a geração de relatórios pós-teste a serem apresentados e entregues aos solicitantes. Neste momento cabe frisar: para que o artigo não se tornasse extenso em demasia, estes autores optaram por apresentar a estruturação do teste e não o detalhamento minuncioso das ferramentas a serem utilizadas em cada etapa, deixando tal aprofundamento como possibilidade em trabalhos futuros.

Na sequência, foram tecidas considerações sobre a adoção de testes de invasão no contexto militar, principalmente no que tange aos aspectos normativos e configuração de equipes de pentesting.

Por fim, em um olhar aproximado, vislumbra-se como benefícios imediatos da implementação de tais testes no meio militar, não só o reforço substancial da proteção cibernética dos ativos de Defesa, mas também a identificação e adestramento de pessoal especializado para atuar no ciberespaço (não só como defensores) ativamente como combatentes cibernéticos iniciados e adaptados nos três tipos de ações cibernéticas básicas demandadas pela Doutrina Militar de Defesa Cibernética brasileira (BRASIL, 2014), quais sejam: ataque cibernético, exploração cibernética e proteção cibernética.

IMPLEMENTATION OF PENTESTS IN SUPPORT TO THE CYBER PROTECTION OF SYSTEMS AND NETWORKS OF INTEREST OF DEFENSE

ABSTRACT: This work has as main objective to present fundamental aspects of Pentests and its implementation in support to the cyber protection of networks and systems of interest to the Defense. In this article we present the current protection scenario, dominated by passive techniques and tools, as well as to defend that the support of offensive security, specific to the pentesting process, may be relevant to the establishment of a more balanced situational awareness about the assets of Defense that one wishes to protect .In order to do this, a bibliographical research was carried out in search of consistent concepts about pentesting, main modalities, applicable methodologies and of characteristics that distance it in understanding of other modalities of security evaluations such as Security Audit and Vulnerability Assessment. Afterwards, we have analyzed the dynamics present in the Pentests, identifying procedures and correlations between each interdependent phase and how each stage influences the result of such tests. Finally, considerations were made regarding the implementation of pentesting in

THE MILITARY CONTEXT, POINTING OUT STRUCTURAL, TRAINING AND TEAM BUILDING PATHS SO THAT THE BENEFITS ARISING FROM THE ADOPTION OF SUCH PRACTICE WOULD NOT BE LIMITED TO COMPLEMENTING THE PROTECTION OF DEFENSE ASSETS, AS INITIALLY PROPOSED, BUT ALSO TO CONTRIBUTE IN A RELEVANT WAY TO THE TRAINING OF THE BRAZILIAN CYBER COMBATANT.

KEYWORD: PENTEST. OFFENSIVE SECURITY. CYBER PROTECTION. CYBER DEFENSE. BRAZILIAN DEFENSE.

REFERÊNCIAS

BERTOGLIO, D. D.; ZORZO, A. F. Um mapeamento sistemático sobre Testes de Penetração. Porto Alegre: FACIN/PUCRS, 2015.

BRASIL. Decreto-lei no 6.703, de 18 dezembro de 2008. Aprova a Estratégia Nacional de Defesa. Presidência da República. Brasília, 2008.

_____. MD31-M-07: Doutrina Militar de Defesa Cibernética. Ministério da Defesa. 1. Ed. Brasília, 2014.

CARDOSO, L.H.F. Anatomia de um ataque cibernético: conhecer e entender para melhor defender os ativos e meios de interesse da Força Aérea Brasilieira. SPECTRUM: Revista do Comando Geral de Operações Aéreas, Brasília, n.20, p.51-57, set. 2017.

CEH. Module 1: introduction to Ethical Hacking Certified Ethical Hacker Course, V.9. Ec-Council. 78p, 2017.

ELEARNSECURITY. How to become a penetration tester. Introduction to a career in IT Security. Whitepaper. 2015.

IAHN, T. S. Teste de Invasão em ambiente de governo. SERPRO. 2018. Disponível em: <http://www.serpro.gov.br/menu/noticias/noticias-2018/testes-de-invasao-em-ambientes-de-governo-1>. Acesso em 03 agosto 2018.

LOSPINOSO, Josh. Fish out of Water: How the military is an impossible place for hackers, and what to do about it. War on the Rocks. 2018. Disponível em :< https://warontherocks.com/2018/07/fish-out-of-water-how-the-military-is-an-impossible-place-for-hackers-and-what-to-do-about-it/>. Acesso em 03 agosto 2018.

OPTRASECURITY. Optra Security. 2018, Disponível em: <https://www.optrasecurity.com.br/>. Acesso em 04 agosto 2018.

ROHR, A. Como brechas em programas são classificadas pelo governo dos eua. G1: Segurança Digital. 2017. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/como-brechas-em-programas-sao-classificadas-pelo-governo-dos-eua.html>. Acesso em 02 agosto 2018.

WEIDMAN, G. Testes de Invasão. São Paulo: 1º Ed. Novatec, 2014.

TOSCH. Basic use of Nmap. Tosch Production. 2011. Disponível em: < https://toschprod.wordpress.com/2011/10/07/basic-use-of-nmap/>. Acesso em 02 agosto de 2018.

Luiz Henrique Filadelfo Cardoso é 2º Sgt especialista em Comunicações (BCO), concluiu o Curso de Formação de Sargentos pela Força Aérea Brasileira (FAB) no ano de 2007, é Bacharel em Sistemas de Informação com ênfase em Análise de Sistemas pela Faculdade de Porto Velho (2011) e pós-graduado em Gestão de Segurança da Informação (2013) e em Inteligência de Segurança (2014) pela Universidade do Sul de Santa Catarina – UNISUL. Também possui o Curso de Guerra Eletrônica pela Força Aérea Brasileira (2013) e o Curso de Guerra Cibernética para Sargentos ministrado pelo Exército Brasileiro (2016). Atualmente exerce a função de Analista de Segurança da Informação. Contato: luizlhfc@fab.mil.br

Lucas Maurício Alves Zigunow é 3º Sgt especialista em Informática (SIN), concluiu o Curso de Formação de Sargentos pela Força Aérea Brasileira (FAB) no ano de 2012, é Técnologo em Redes de Computadores pela Universidade Estácio de Sá (2017), cursando pós-graduação em Computação Forense e Perícia Digital pelo Instituto de Pós-Graduação e Graduação (IPOG) e mestrando em Segurança dos Sistemas de Informação e das Redes pela Universidade de Brasília (UnB). Também possui, Curso de Guerra Cibernética para Sargentos ministrado pelo Exército Brasileiro (2017), Certificação Ethical Hacker v9 pela EC-Council e outros cursos na área de TI. Atualmente exerce a função de Analista de Segurança da Informação. Contato: lucaslmaz@fab.mil.br

CICAD.II.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

ANÁLISE DE ZONAS DE SILÊNCIO PARA TRANSMISSÕES EM HF

Antonio Anderson Silva Marques
Pós-graduado em Gestão de Sistemas Táticos de Comando e Controle

RESUMO: Estudos da propagação em HF colaboram para retirar territórios fronteiriços de possíveis "zonas de silêncio" na comunicação rádio, assim viabilizando um comando e controle mais eficaz. Pelotões Especiais de Fronteira (PEF) encontram-se muitas vezes em locais de baixa infraestrutura, onde não há cabeamento estruturado, Estações Rádio-Base (ERB) de operadoras de telefonia ou enlaces via micro-ondas. Este manuscrito verificou as limitações da propagação rádio em linha de visada e através de ondas ionosféricas, identificando as particularidades de cada tipo de onda, levando-se em conta o ambiente de selva e os equipamentos disponíveis para estas tropas. Os resultados apontam que enlaces em linha de visada terão baixa efetividade neste ambiente, porém a propagação pela ionosfera pode ser adotada como uma solução viável, desde que os equipamentos rádio disponíveis sejam utilizados de forma criteriosa, escolhendo as frequências, antenas e configuração correta do equipamento.

Palavras-chave: Propagação. HF. NVIS. Rádio. Enlaces.

INTRODUÇÃO

A utilização de transmissões em High Frequency (HF) possui uma ampla aplicabilidade para a segurança da infraestrutura crítica de telecomunicações. Em especial para as Forças Armadas (FA), há diversos contextos operacionais onde este tipo de comunicação pode ser empregado, entre eles as comunicações em ambiente de selva na Amazônia ou para transmissões entre embarcações.

AGARD (1990) aponta que a ionosfera é uma região composta por íons livres em quantidade suficiente para afetar as propriedades de ondas eletromagnéticas, entretanto esclarece que a densidade de elétrons pode sofrer grandes variações de acordo com a região geográfica.

Mayor (2016) cita que há três tipos mais comuns de propagação para as transmissões em HF que podem sensibilizar o receptor: as ondas diretas, que se irradiam diretamente do transmissor para o receptor, as ondas terrestres e as ondas ionosféricas, que refratam nas camadas da ionosfera e retornam para o solo, provendo um grande alcance para as comunicações.

Elementos receptores situados além do limite do alcance das ondas diretas e terrestres terão que contar com o sinal advindo da ionosfera. O limite entre o alcance das ondas diretas e o das ondas ionosféricas compreende uma "zona de silêncio", onde elementos importantes da tropa podem estar sem comunicação.

Determinados ambientes operacionais sempre representaram um desafio para as comunicações. O Exército Brasileiro em especial possui permanentemente vários pelotões de fronteira (PEF) situados nos limites no território nacional. Estes pelotões estão relacionados à "estratégia de presença" do Exército Brasileiro na região fronteiriça, representando o primeiro contato contra uma possível hostilidade externa, além da finalidade de "vivificação" da faixa de fronteira, sendo núcleos embrionários de desenvolvimento social e ocupação de áreas ora inertes (MIRANDA, 2012).

Embora haja comunicações satelitais para alguns destes pelotões, este tipo de enlace ainda não está plenamente disponível para as tropas brasileiras, tendo em vista seu alto custo e prioridade de alocação de banda para finalidades próprias do governo brasileiro.

Tropas brasileiras empregadas em ambientes operacionais de selva necessitam de comunicações estáveis para o cumprimento de suas mais diversas missões. Os equipa-

mentos disponíveis para estas tropas, sendo Rádios definidos por software, possuem uma boa capacidade de transmissão de dados e alcance, tendo em vista as informações disponibilizadas nos manuais dos fabricantes. Assim, este projeto teve como metas fundamentais:

a) verificar o alcance de ondas diretas e terrestres em diferentes tipos de transmissão dos equipamentos rádio HF atualmente disponíveis;

b) observar as perturbações na ionosfera que impactam no seu plasma energético, a fim de compreender quais as melhores frequências de acordo com a região e o horário de transmissão;

c) estimar o raio das zonas de silêncio visando missões nas proximidades do PEF que não possam ser cobertas por transmissões em visada direta.

1 METODOLOGIA

Foi realizada uma pesquisa bibliográfica sobre os temas: características da atmosfera, no tocante ao plasma ionosférico; propagações por ondas diretas e ionosféricas e análise das características dos equipamentos disponíveis para tropas brasileiras, como ângulo de partida, sensibilidade para recepção e diretividade das antenas.

Foram utilizados artigos, dissertações, teses e livros disponíveis na literatura especializada. Assim como as recomendações da União Internacional de Telecomunicações (UIT).

Posteriormente, foram realizados os cálculos de propagação eletromagnética, visando determinar o alcance máximo de um enlace via ondas diretas e a região aproximada do primeiro “salto” após refração na ionosfera, de modo a ter uma delimitação da zona de silêncio.

1.1 FORMAS DE PROPAGAÇÃO

Wivlet et al. (2015) aponta que as propagações ionosféricas podem funcionar com eficácia para um raio de 150 km a partir da fonte emissora. Especialmente na faixa do espectro eletromagnético de 3 e 10 MHz, pois esta faixa de frequência sofre o fenômeno da refração na ionosfera, possibilitando seu retorno ao solo.

Ressalta-se que tamanha área de cobertura possui dificuldade acentuada de obter boa relação sinal-ruído nas estações receptoras com faixas de frequência de valor mais elevado, tendo em vista o relevo e a vegetação características do ambiente de selva. Faixas acima de 30 MHz necessitam, na maioria dos casos, de visada direta para sua propagação, o que levaria a adoção de inúmeros repetidoras em locais isolados e de difícil acesso para as tropas.

Para a determinação da probabilidade de enlace utilizando ondas ionosféricas foram realizados cálculos levando-se em conta o ângulo de partida e o tipo de antena, sendo posteriormente analisados no software VOACAP (Voice of America Coverage Analysis Program for HF Propagation Prediction and Ionospheric Communications Analysis). Determinados parâmetros foram obtidos através de estudos de ionogramas, em especial utilizando a ionossonda de Boa Vista, por ser esta a sonda mais próxima dos pelotões especiais de fronteira.

Já para a propagação em visada direta foram realizados cálculos em situações típicas de comunicações entre pequenos escalões militares. A falta de estruturas fixas - torres, mastros elevados, antenas de ganho elevado etc. - torna este tipo de comunicação tática um desafio no ambiente de selva.

Devido a obstruções da vegetação e do perfil topográfico do próprio terreno, é comum haver muitas perdas no percurso até a estação receptora. Estas perdas foram observadas utilizando o modelo de propagação Longley-Rice, que estima as perdas por difração

em um enlace levando em conta vários fatores como as irregulares do terreno, condutividade do solo, curvatura da terra, distância entre as estações etc.

Para os enlaces com o modelo de propagação Longley-Rice, foi utilizado o software Radio Mobile, levando-se em conta os tipos de antena que seriam utilizados no ambiente de selva.

2 DISCUSSÃO E RESULTADOS

2.1 PROPAGAÇÃO VIA VISADA DIRETA

Medeiros (2011) aponta que enlaces em visibilidade, ou visada direta, exigem potência significativa para uma comunicação a dez ou mais quilômetros. Em situações onde há obstáculos presentes, essa necessidade de potência pode se tornar ainda maior, tendo em vista a obstrução das zonas de Fresnel.

Os receptores táticos utilizados pelo Exército Brasileiro atualmente, da empresa Harris, possuem uma sensibilidade da ordem de -90 dBm (HARRIS, 2017). Visando ilustrar as dificuldades deste tipo de enlace na selva, podemos adotar os seguintes valores para análise:

QUADRO 1 Características de um enlace em ambiente de selva

Características do Enlace	Valores
Distância entre uma companhia e um pelotão em missão real em ambiente de selva.	30 km
Frequência	100 MHz
Potência de Transmissão	10 W
Ganho das Antenas	-5 dBi
Perdas por acoplamento das antenas	- 2 dBi
Ruído na recepção	-113 dBm

Fonte: o autor, 2018.

Medeiros (2011) cita que a atenuação do espaço livre pode ser obtida, para D em quilômetros, e F em MHz, por:

L [dB] = 36,57 + 20 log (*D* * 0,62) + 20 log *F* **(1)**

L = 36,57 + 20 log 18,64 + 20 log 100;

L = 36,57 + 25,41 + 40;

L = 101,99 dB

A potência transmitida em dB será:

Pt = 10 log 10 = 10 dBW

A potência recebida será então:

Pr [dBW] = 10 dBW – 5 dBi – 5 dBi – 101,99 dB – 4 dBi = - 105,99 dBW

Convertendo dBW para dBm:

Pr [dBm] = - 105,99 dBW + 30 = - 76 dBm

O valor de – 76 dBm apresenta uma potência recebida satisfatória, porém, as situações táticas apresentadas no ambiente de selva exigem muitas vezes a transposição de obstáculos. O impacto das obstruções, também chamadas de perdas por difração, pode ser inicialmente avaliado pelo cálculo das Zonas de Fresnell, onde o primeiro raio, ou primeira zona, pode ser descrito como:

$$\boldsymbol{R1\,[m] = 17,32\sqrt{\frac{D}{4f}}} \qquad (2)$$

D = distância total do enlace;

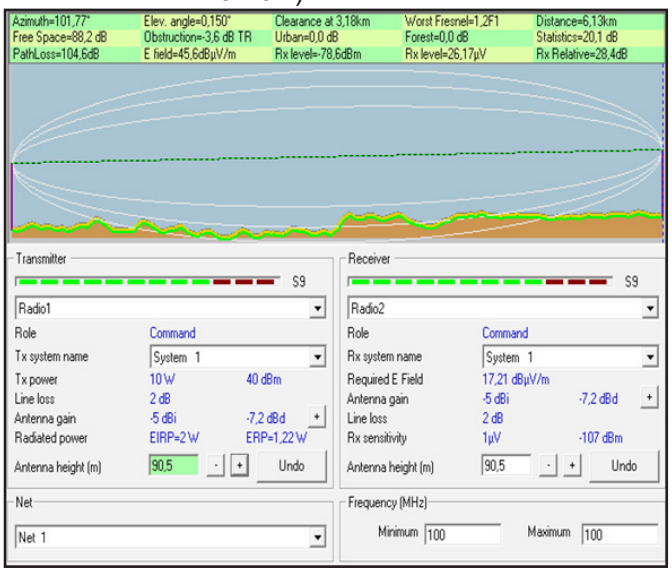
f = frequência.

Analisando a equação do raio de Fresnell, pode-se observar que R1 é inversamente proporcional à frequência, assim, conforme desejarmos transmitir em frequências acima de 30 MHz, haverá um impacto cada vez maior das obstruções do terreno. Em simulações realizadas no software Radio Mobile, há perdas da ordem de 30 dBm devido às condições do terreno, conforme figura 1 e 2.

A figura 1 apresenta uma situação hipotética do uso de duas torres instaladas na região do 5o Pelotão Especial de Fronteira Maturacá (00o37'26''N, 66o05'48''W), 90 metros acima do nível do solo, configurando assim um enlace em linha de visada. Porém, conforme já citado neste manuscrito, a utilização dos equipamentos em situações táticas muitas vezes exige transmissões onde as antenas estarão em baixas alturas, conforme a figura 2. Quan-

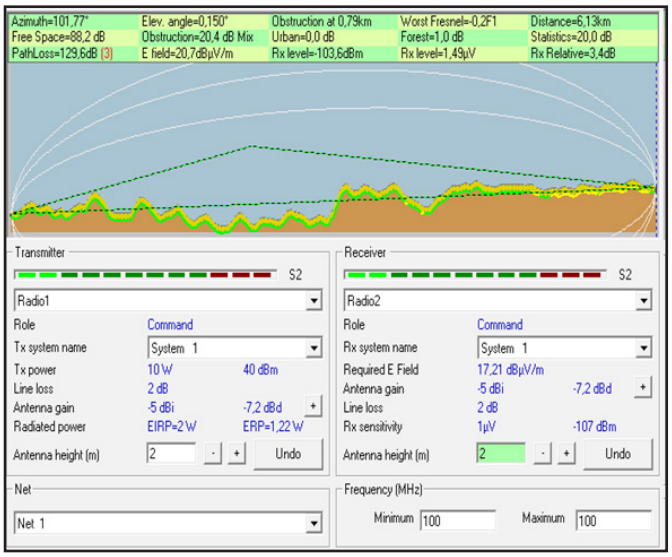
do isto ocorre, há obstrução de parte relevante da primeira zona de Fresnel, aumentando a perda no percurso.

FIGURA 1 Enlace em linha de visada utilizando torres (perda no percurso de 104 dB)



Fonte:o autor, 2018.

FIGURA 2 Enlace em linha de visada na altura do solo (perda no percurso de 129 dB)



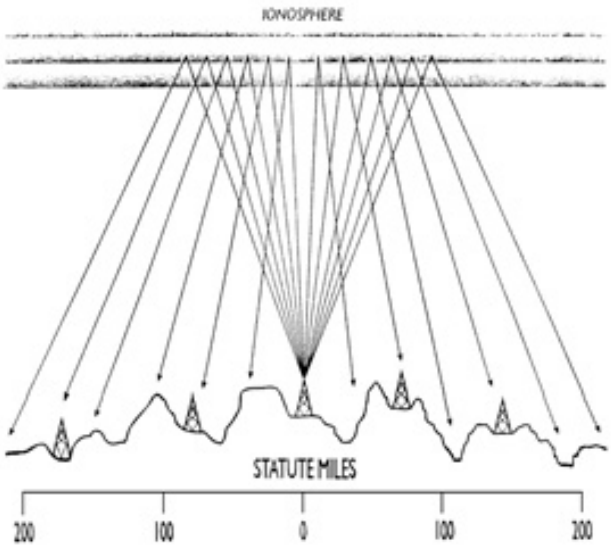
Fonte: o autor, 2018

2.2 PROPAGAÇÃO VIA ONDAS ESPACIAIS

Uma alternativa para as perdas em linha de visada é o uso de frequências entre 3 e 12 MHz, também chamadas de NVIS, Near Vertical Incident Skywave. Wallace (1992) cita diversos exemplos bem sucedidos para o uso de NVIS em campo aberto. Sendo relevante a escolha correta da frequência, o tipo de antena que será utilizado e de seu ângulo de partida.

A forma de cobertura do NVIS assemelha-se a um guarda-chuva nas proximidades da antena transmissora, conforme pode ser observado na figura 3. Este tipo de transmissão exige ângulos de partida elevados, que possam alcançar a ionosfera e serem refratados de volta para o solo em uma área que dificilmente um enlace em visada direta poderia alcançar.

Porém há limitações para este tipo de transmissão que ainda podem ocasionar zonas de silêncio nas proximidades da antena transmissora. Estas limitações estão relacionadas não somente com o ângulo de partida



mas também com a frequência que se deseja transmitir em um região específica.

FIGURA 3 Propagação em NVIS

Fonte: NVIS-TUGA (2010).

3.2.1 Ionossondas

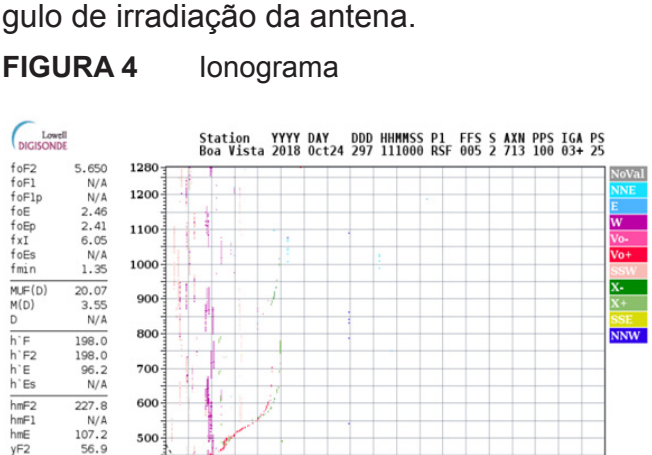
Sendo afetadas por diversos fatores naturais, o estudo de propagações ionosféricas é facilitado com o uso das ionossondas. Estes dispositivos estão localizados em diversas cidades ao redor do mundo, medindo a “altura” da ionosfera e sua densidade de elétrons por camada.

Wivlet et al. (2015) afirma que através das ionossonda é possível determinar a frequência crítica, ou a frequência de plasma, de uma camada, que seria a frequência mais alta de irradiação que retornou para a ionossonda

em uma propagação vertical na direção do zênite (ângulo de incidência zero sobre a Normal da Terra). A figura 4 apresenta as informações principais que devem ser lidas em um ionograma. O eixo horizontal apresenta as frequências na faixa do HF, o eixo vertical a altura virtual da ionosfera para aquele momento. As curvas indicam o comportamento da frequência em cada altura, sendo a curva vermelha a mais relevante, que são as Ondas Ordinárias. Para fins de cálculo de enlace, a curva verde, Ondas Extraordinárias, pode ser ignorada.

"Fo" representa a frequência crítica de operação para determinada camada da ionosfera, sendo o parâmetro mais relevante "foF2", pois este aponta o valor de frequência para a camada mais densa, a camada F2. "MUF" representa a Máxima Frequência Utilizável, porém este parâmetro está condicionado ao ângulo de irradiação da antena.

FIGURA 4 Ionograma



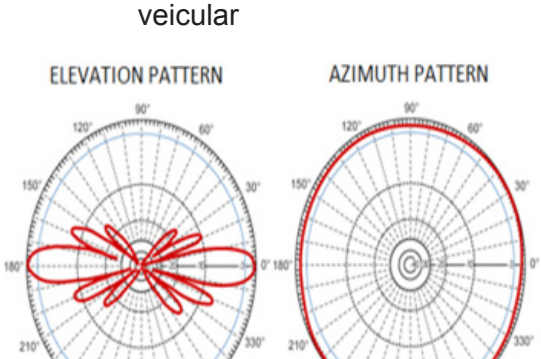
Fonte: GIRO (2018)

2.2.2 MUF

Martyn (1935) demonstrou que: MUF = fc*secθ, sendo fc a frequência crítica e θ o ângulo de incidência na ionosfera. Esta relação, derivada da lei de Snell, mostra que à medida que o ângulo de incidência é ampliado, a MUF aceitará valores maiores de frequência. Este ângulo de incidência implicará no alcance da propagação.

As antenas utilizadas em viaturas por exemplo, do tipo vertical, não terão ângulo de partida suficiente para refração na atmosfera. Observando o lóbulo de radiação de antenas verticais, conforme figura 5, é possível verificar que sua maior incidência de radiação será em ângulos de partida baixos. Propagações acima de 30º, pelo tamanho reduzido dos lóbulos, terão baixa probabilidade de alcançar uma estação receptora.

FIGURA 5 Diagrama de irradiação de antena veicular



Fonte: Harris (2017)

A tabela 1 apresenta os diversos ângulos de incidência para a frequência crítica de 5,65 MHz, utilizando como referência a altura virtual da ionosfera de 198 km, conforme obtido no ionograma da figura 4. Os cálculos da tabela 1 indicam, por exemplo, que transmitir em uma frequência acima de 5,89 MHz para cobrir uma distância menor que 25 Km em NVIS levará a perda do sinal, pois o mesmo não refratará nas camadas da ionosfera. De forma análoga, uma propagação de 6,03 MHz para uma estação receptora a 100 km deverá ter seu ângulo de incidência limitado a 12,8°, ou seu ângulo de partida deverá ser no máximo 77,2° (90 - 12,8), caso esta frequência assuma ângulos de partidas maiores, ultrapassará a atmosfera e não retornará para a Terra.

TABELA 1 Ângulos de incidência na ionosfera

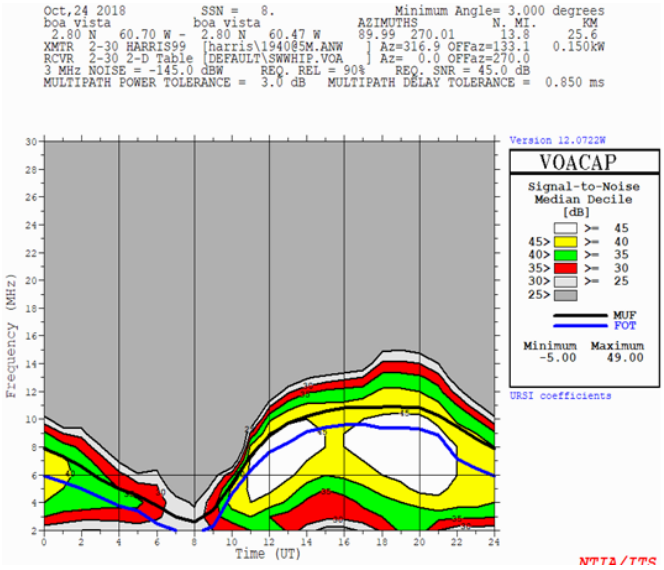
θ (graus)	fc (Hz)	MUF (Hz)	D (km)
0,3	5,65	5,88	2
0,7	5,65	5,88	5
1,0	5,65	5,88	8
1,8	5,65	5,88	14
3,3	5,65	5,89	25
6,5	5,65	5,92	50

θ (graus)	fc (Hz)	MUF (Hz)	D (km)
9,7	5,65	5,96	75
12,8	5,65	6,03	100
15,9	5,65	6,11	125
21,7	5,65	6,33	175
32,0	5,65	6,46	200
34,3	5,65	6,60	225
32,0	5,65	6,93	275
34,3	5,65	7,12	300
36,5	5,65	7,31	325
40,4	5,65	9,04	375
42,3	5,65	10,65	400
69,9	5,65	17,08	1200

Fonte: o autor, 2018.

Ao confrontar este resultado com o software de predição VOACAP, é possível observar que a aplicação não traz as informações mais precisas, visto que apontou como MUF o resultado de 7,33 MHz para o mesmo horário, o que levaria possivelmente à falha no enlace, conforme figura 6.

FIGURA 6 Simulação de propagação no VOACAP



Fonte: o autor, 2018.

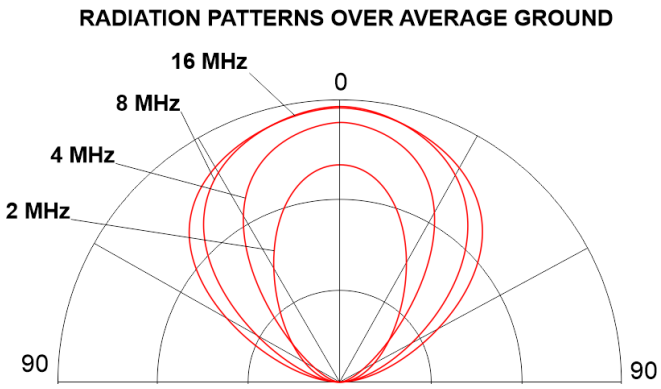
Utilizando a relação trigonométrica da secante, os resultados da tabela 1 foram obtidos através de:

$$MUF\ [Hz] = fc\sqrt{(1+\frac{D}{2H})} \quad (5)$$

Onde D = distância do enlace; H = altura virtual da camada mais densa da ionosfera.

Aplicando a equação 3 para um enlace de 1200 km obtemos como resultado uma MUF de 17,08 MHz e ângulo de incidência de 69,9°, ou ângulo de partida de 20,1°, porém observando o diagrama de irradiação da antena RF-1941 (dipolo), da empresa Harris, na figura 7, é possível observar que este ângulo possui baixa energia irradiada, o que levará a falha no enlace.

FIGURA 7 Radiação da antena RF-1941 (dipolo)



Fonte: Harris (2017).

CONCLUSÃO

Ao realizar estudos de propagação em ambiente de selva, é possível verificar a incidência de muitas perdas por difração no percurso do enlace. Conforme simulações realizadas com o modelo de propagação Longley-Rice, as perdas podem alcançar valores da ordem de 30 dBm, o que inviabiliza a maioria das tentativas de estabelecer comunicações em distâncias comuns para tropas no terreno.

Uma possível solução para este tipo de problema seriam antenas direcionais táticas, embora ainda haja perdas por difração na primeira zona de Fresnell - o raio da primeira zona não é alterado pela diretividade da antena - o ganho irradiado em um determinado azimute poderia compensar estas perdas.

De outra forma, a propagação em NVIS apresenta-se como uma solução para as

comunicações. Utilizando as frequências críticas dos ionogramas de cidades próximas à região de interesse, no caso em análise Boa Vista, é possível determinar uma lista de frequência para se operar em variadas distâncias.

Cabe ressaltar que este tipo de comunicação se adequa muito bem para comunicações que não exijam largura de banda elevada, que é uma variável diretamente proporcional à frequência escolhida. Caso se deseje operar em frequências mais elevadas, visando transmissão de dados, o sistema terá um ângulo crítico a ser limitado, caracterizando o padrão "guarda-chuva" da cobertura.

Sendo NVIS uma forma de propagação eficiente, torna-se relevante mais pesquisas em como adaptar antenas veiculares a este tipo de propagação. Atualmente, para tropas militares brasileiras, a melhor solução para NVIS é a utilização de antenas do tipo dipolo, devido ao seu lóbulo de irradiação cobrir toda a região nas proximidades do zênite.

Na data de conclusão deste trabalho, as manchas solares estavam com seus valores muito reduzidos, dificultando sobremaneira o aumento da densidade de elétrons da ionosfera, o que levou a frequências críticas muito baixas. Como forma de contornar este problema, sugere- se a utilização de enlaces digitais somente, tendo em vista que estes exigem uma menor relação sinal ruído para satisfazer a qualidade pretendida (Medeiros, 2011).

Novos estudos podem ser realizados utilizando os equipamentos táticos partindo dos dados das situações simuladas, verificando por exemplo, se é possível aumentar as frequências além da MUF com a digitalização do sinal ou obter uma melhor relação sinal ruído com tipos diferentes de modulação.

Os PEF geralmente encontra-se em locais de baixa infraestrutura, onde muitas vezes não há cabeamento estruturado, Estações Rádio-Base (ERB) de operadoras de telefonia ou até mesmo, a possibilidade de enlace via micro-ondas, devido a longa distância, permeada de rios e matas, entre estes pelotões e suas sedes logísticas.

Estudos da propagação em HF colaboram para retirar estes territórios fronteiriços de possíveis zonas de silêncio, assim viabilizando transmissões de dados e fonia para tropas que dependerão muitas vezes exclusivamente

deste meio de comunicação. Levando-se em conta ainda que, diversas vezes, estes pelotões realizarão missões em locais distantes de suas sedes, o que fortalece a necessidade de estudo das propagações em HF visando garantir as comunicações também neste tipo de missão.

ANALYSIS OF SILENCE ZONES FOR HF TRANSMISSIONS

Abstract: HF propagation studies collaborate to remove frontier territories from possible "silent zones" in radio communication, thus enabling more effective command and control. Special Border Platoons (PEFs) are often located in low-infrastructure locations, where there is no structured cabling, radio base stations (ERB) from telephone operators or links via the microwave. This manuscript verified the limitations of HF propagation in line of sight and through ionospheric waves, identifying the particularities of each type of wave, taking into account the environment of the jungle and the equipment available for these troops. The results indicate that line- of-sight links will have low effectiveness in this environment, but propagation through the ionosphere can be adopted as a viable solution, provided that the available radio equipment is used in a judicious way, choosing the frequencies, antennas and correct configuration of the equipment.

Keywords: Propagation, HF, NVIS, radio, links

REFERÊNCIAS

Advisory Group for Aerospace Research and Develpment (AGARD). AGARD-AG- 326 - Radio Wave Propagation Modeling, Prediction and Assessment. NORTH ATLANTIC TREATY ORGANIZATION. 1990.

BISPO, M. N., Análise do Canal Ionosférico de Rádio-Propagação na Faixa de HF, Dissertação de Mestrado, IME, Rio de Janeiro, 2000.

BOITHIAS, L., Radio Wave Propagation, Mc – Graw Hill Book Company, London, 1987. União Internacional de Telecomunicações.

CANAVITSAS, A. A. C., Otimização de Redes de Radiocomunicações em HF, Dissertação de Mestrado, IME, Rio de Janeiro, 2000.

GIRO. GLOBAL IONOSPHERE RADIO OBSERVATORY. DIDBase. Acesso em 24/10/2018. Disponível em http://giro.uml.edu/.

GIUSEPPE, V. A. Análise do Comportamento da Ionosfera a Partir de Medidas dm HF. Instituto Militar de Engenharia. Dissertação De Mestrado. 2003

HARRIS. Harris Falcon III RF-7800V-HH. NEW YORK, 2017.

MARTIN. D. F. D. F. Martyn, R. O. Cherry, and A. L. Green, Long-distance observations of radio waves of medium frequencies. Proc. Phys. Soc., vol. 47, no. 2, pp. 323–340, Mar. 1935.

MAYOR, R. M. ANT – Antenas e Propagação. Instituto Federal de Educação, Ciência e Tecnologia Campus São José – Santa Catarina. 2016.

MEDEIROS, J. C. de O. Princípios de Telecomunicações. 3 ed. São Paulo. Érica, 2011.

MIRANDA, W. D. DEFESA E EXÉRCITO NA AMAZÔNIA BRASILEIRA: Um estudo sobre a constituição dos Pelotões Especiais de Fronteira. Dissertação de Mestrado. UFPA. Belém. 2012.

NVIS-TUGA. NVIS Tático. 2010. Acesso em 24/10/2018. Disponível em http://nvis- tuga.blogspot.com/2010/11/nvis- tactico.html.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. Recommendation ITU-R P. 533-7 – HF Propagation Prediction Method, ed UIT 2001 18 p.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, Recommendation ITU-R P 373-7 – Definitions of Maximum and Minimum Transmission Frequencies, Question ITU- R 213/3, ed UIT 1995 1p.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, Recommendation ITU-R BS.705-1 – HF transmitting and receiving antennas characteristics and diagrams. ed UIT 1995 138p.

WIVLET, B. A. et al. Near Vertical Incidence Skywave Propagation: Elevation Angles and Optimum Antenna Height for Horizontal Dipole Antennas. 2015. IEEE Antennas and Propagation Magazine, Vol. 57, No. 1, February 2015.

O autor é graduado em Ciências Militares pela Academia Militar das Agulhas Negras. Mestrando em Engenharia Elétrica pela Universidade de Brasília. Possui cursos na área de Rádios definidos por software, Sistemas Satelitais e Comando e Controle. Foi instrutor na Academia Militar das Agulhas Negras. Atualmente, exerce a função de instrutor na Escola de Comunicaçoes. Pode ser contactado através do e-mail silvamarques.anderson@eb.mil.br.

CICAD.II.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

ATAQUES CIBERNÉTICOS E MEDIDAS GOVERNAMENTAIS PARA COMBATÊ-LOS

Washington Rodrigues da Silva[1], Jorge Madeira Nogueira[2]
Mestre em Economia da Defesa[1], Doutor em Economia Regional[2]

RESUMO: O uso do espaço cibernético cresce a cada dia. Os ataques cibernéticos acompanham esse crescimento, apresentando-se como ameaça constante e mutável. Esses ataques comprometem a confidencialidade, integridade e/ou disponibilidade de dados, sistemas e serviços, com reflexos negativos em variados setores da economia. Objetivou-se estudar os ataques cibernéticos, seus riscos e como são tratados por governos ao redor do mundo e no Brasil. Foram utilizadas fontes secundárias de pesquisa bibliográfica. Identificou-se que o Brasil se encontra em nível intermediário de segurança cibernética, segundo critérios da União Internacional de Telecomunicações. Além de que a maior parte dos ataques cibernéticos sofridos no Brasil reportados ao CERT.br originam-se no próprio país, o que pode ser uma consequência da falta de leis específicas e da sensação de impunidade pelos infratores. E, que houve um início de aproximação entre órgãos do governo e da iniciativa privada para colaboração na melhoria da capacidade de proteção cibernética no Brasil.

Palavras-chave: Ataques cibernéticos. Brasil. Defesa.

INTRODUÇÃO

As facilidades proporcionadas pelos sistemas de tecnologia da informação e comunicação (TIC) trouxeram consigo oportunidades para a exploração de um novo ambiente, o chamado espaço cibernético, para usos benéficos ou prejudiciais. Nesse contexto, as novas TIC criaram desafios e efeitos negativos. Por exemplo, por meio delas, surgiram novas possibilidades de explorações para fins de crimes financeiros, espionagem industrial e até ataques entre Nações. Nesse cenário, governos e instituições de diversos países passaram a tomar providências para protegerem-se. Como o resto do mundo, o Brasil tem, diante de si, semelhantes desafios.

Do exposto, levantou-se a problemática: quais são os impactos de ataques cibernéticos? Em virtude da elevada amplitude do tema, buscou-se delimitar o estudo conforme segue: este trabalho tem o objetivo de estudar os ataques cibernéticos, seus riscos e como são tratados por governos ao redor do mundo e no Brasil.

Assim, o presente trabalho faz-se relevante por destacar o quão presentes e danosos são os ataques cibernéticos e destacar a importância da atuação do Estado, por meio de políticas públicas e ações para combater essa ameaça.

Este artigo é dividido em 4 (quatro) seções, além desta introdução e das conclusões. Na primeira, é tratado sobre o espaço cibernético e são os tipos de ameaças cibernéticas. A segunda seção aborda as dimensões econômicas de ataques cibernéticos. A terceira aborda como outros países estão enfrentando o atual cenário de ataques cibernéticos e quais estruturas foram criadas para tal. Na quarta seção, há semelhante abordagem sobre como está o Brasil nesse cenário.

Metodologicamente, utilizou-se dados de fontes secundárias, obtidos por meio de uma pesquisa bibliográfica aplicada. Buscou-se dados e informações em livros especializados e artigos científicos, sítios oficiais de órgãos como os brasileiros Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br), Exército Brasileiro (EB) e Ministério da Defesa (MD); os estadunidenses Federal Bureau of Investigation (FBI), The Council of Economic Advisers (CEA), os britânicos National Cyber Security Centre (NCSC) e o UK Cabinet Office, a página do Office of Prime Minister, da Austrália e da União Internacional de Telecomunicações (ITU, sigla em inglês), com sede na Suíça. Além de portais de jornais de grande circula-

ção no Brasil como o Valor Econômico.

Ademais, a pesquisa por fontes incluiu conteúdos redigidos em língua portuguesa, inglesa e espanhola, publicadas a partir do ano 2000, dando-se preferência a publicações recentes, principalmente a partir de 2013. Dessas, a maior parte das fontes de referências obtidas do exterior são oriundas dos Estados Unidos da América (EUA) por haver maior disponibilidade de estudos em fontes abertas.

1 AMEAÇAS CIBERNÉTICAS: SUAS INÚMERAS DIMENSÕES

1.1 O ESPAÇO CIBERNÉTICO

O surgimento da internet foi o primeiro passo para o atingimento do grau de compartilhamento de informações vivenciados atualmente. Nesse contexto, surge uma nova dimensão, o espaço cibernético. Esse espaço apresenta, segundo Oliveira et al. (2017), três características: dimensão intangível e abstrata; considerado importante desde o início de sua existência; e transversal, esta última em consonância com Ventre (2011), o qual adiciona que o espaço cibernético permeia todos os espaços geográficos, permitindo controlar desde satélites e radares marítimos até metrôs em grandes cidades, assim, as ações geradas no campo virtual são capazes de criar consequências no mundo real.

O espaço cibernético e a internet apresentam semelhanças, contudo são distintos, apesar de haver discordância. Cebrowski (2004) afirma que o espaço cibernético é maior do que a internet. Autores como Carvalho (2011) e Oliveira et al. (2017) concordam com essa concepção e incluem que o espaço cibernético é composto por dispositivos computacionais, conectados em redes ou não, com trânsito ou armazenamento de informações. Há, ainda, autores que incluem os usuários na composição do espaço cibernético, como é o caso de Klimburg (2012), o qual afirma que “o espaço cibernético é mais que internet, inclui não somente hardware, software e sistemas informacionais, mas também pessoas e suas interações sociais nas redes de computadores”.

1.2 TIPOS E INSTRUMENTOS DE AMEAÇAS NO ESPAÇO CIBERNÉTICO

As principais ameaças são os ataques cibernéticos. Klinburg (2012) afirma que esse não é um termo internacionalmente definido, havendo diferenças substanciais entre a definição do governo estadunidense e de outros países. A definição mais genérica de ataque cibernético é que se trata de uma tentativa maliciosa premeditada de ataque para quebrar a confidencialidade, integridade ou disponibilidade de informações existentes em computadores ou redes computacionais.

O governo dos EUA trata ataques cibernéticos como atividade cibernética maliciosa e as definem da seguinte forma:

> Atividade cibernética maliciosa é qualquer atividade, desautorizada ou em desacordo com a lei dos EUA, que busca comprometer ou prejudicar a confidencialidade, integridade ou disponibilidade de computadores, sistemas de informação ou comunicações, redes, infraestrutura física ou virtual controlada por computadores ou sistemas de informação, ou as informações nele contidos (CEA, 2018, p. 2).

Já o Ministério da Defesa do Brasil entende como ataque cibernético quaisquer “ações que objetivam interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente” (BRASIL, 2014a, p. 23).

Os agentes cibernéticos são classificados de acordo com os fins de suas atuações. O termo hacker, bastante utilizado cotidianamente como uma generalização de usuários criminosos, não significa exatamente isso. Ramalho Terceiro (2002) aponta hacker como alguém possuidor de grande habilidade em computação. Já os crackers são hackers que utilizam seus conhecimentos para atacar computado-

res, utilizando seus potenciais cognitivos para cometer atos ilícitos, ou seja, os criminosos são, essencialmente, os crackers. Apesar da diferença entre os termos, o termo hacker será utilizado neste artigo indistintamente.

Raposo (2007) destaca a existência de um grupo formado por hackers com motivações políticas ou religiosas, contratados por extremistas com o objetivo de realizarem ataques para geração de pânico, mortes, acidentes, contaminação ambiental ou perdas econômicas. Esses hackers são denominados de terroristas cibernéticos. The Council of Economic Advisers, um órgão do governo estadunidense, ratifica esse conceito classificando esses indivíduos que efetuam ataques cibernéticos por razões ideológicas como hacktivistas (CEA, 2018).

Há diversas formas com as quais os atacantes cibernéticos podem buscar seus objetivos. Caldas (2016) afirma que parte considerável das ações criminosas em redes computacionais são praticadas com uso de softwares maliciosos, conhecidos por malwares e os define como programas criados com a intenção de se infiltrar em um sistema de computador alheio de forma ilícita, para causar danos, alterações ou roubo de informações (confidenciais ou não).

Um dos elementos usualmente presentes em ataques cibernéticos são os vírus. Sikorski e Honing (2012) apresentam vírus e worms como tipos de malwares. Easttom (2016) explica que, por definição, os vírus são programas que se autorreplicam e possuem capacidade de rápida propagação. O vírus de computador, análogo ao vírus biológico, necessita de uma aplicação hospedeira para se replicar e infectar outros sistemas.

Outra ferramenta de ataque cibernético são os vermes, conhecidos no meio cibernético como worms. Gaspar (2007) diferencia os worms dos vírus pois não necessitam de um portador para se replicarem. Eles se autorreplicam, espalhando-se de um computador para outro. Os vermes exploram as vulnerabilidades e utilizam quaisquer mecanismos para se propagarem como, por exemplo, e-mails, serviços de internet, compartilhamento de arquivos, mídias removíveis, entre outros.

Os ataques cibernéticos podem ocorrer de diversas outras formas, como Cavalos de Tróia, backdoors, botnets, spywares, phishing, spear phishing, entre outros. Havendo constante surgimentos de novas formas de ataques, segundo o FBI (2018), um desses que está atualmente entre os mais incidentes é o ransomware. Conforme o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br), esse consiste em um tipo de malware que impede o acesso a arquivos digitais valiosos, com isso, os criminosos cobram um resgate para tornar os dados acessíveis novamente (CERT.br, 2018a).

Como o ser humano é parte do espaço cibernético, suas vulnerabilidades devem ser consideradas. Sobre esse tema, Singer e Friedman (2014) afirmam que é justamente o fator mais débil, pois permite várias formas de ataques em razão de procedimentos inadequados.

Uma das possíveis formas de atuação sobre os usuários é a Engenharia Social. Para Pais et al. (2013), a maior fonte de risco para a segurança são as vulnerabilidades dos indivíduos que compõem uma organização visada. Em razão da simplicidade e engenho, a Engenharia Social é a maneira mais fácil e eficaz de um atacante superar os obstáculos impostos pelos sistemas de segurança.

Oppermann (2013) reforça a ideia de que até usuários frequentes da internet e sabedores da existência de malwares cometem erros primários como clicar em links desconhecidos em rede sociais, e-mails ou em mensagens recebidas em aplicativos de conversação em smartphones.

1.3 ATAQUES CIBERNÉTICOS CONTRA A CONFIDENCIALIDADE

Os ataques cibernéticos contra a confidencialidade possuem, em geral, o objetivo

de conceder, ao atacante, acesso a dados que lhes são negados.

Vianna e Fernandes (2015) destacam que países como Brasil, EUA e Alemanha foram expostos a ações de vigilância e espionagem cibernética, comprometendo a privacidade de pessoas e organizações e, quiçá, até as soberanias dessas nações. Esses não são os únicos, ataques cibernéticos com o fim de espionagem ocorrem em todas as regiões onde houver conteúdos passíveis de gerar algum benefício, seja financeiro, político ou outro qualquer.

Ainda segundo Vianna e Fernandes (2015), em 2013, a situação conhecida como caso Snowden foi um marco emblemático por revelar a atuação do governo dos EUA em espionagem de dados, dentro e fora do seu território. Nesse sentido foi exposto como o governo dos EUA obtinha acesso a e-mails e outros arquivos eletrônicos de usuários, por meio de empresas como Google, Microsoft e Facebook. Dentre esses, estavam a Presidência do Brasil e empresas como a Petrobras.

O peso dos ataques contra confidencialidade tem mais relação com a importância da informação obtida do que com os sistemas computacionais. Assim, a perda da confidencialidade pode gerar instabilidades diplomáticas, como ocorreu no caso Snowden entre o governo dos EUA e os dos países por eles espionados.

A quebra de sigilo sobre conhecimentos restritos, como propriedade intelectual, projetos, tecnologias, know how e afins é a maior ameaça para os setores industriais, acadêmicos e de pesquisa, desenvolvimento e inovação (P&DI), uma vez que neles a informação possibilita a criação de riquezas de elevado valor agregado.

É comum haver elevados níveis de precauções como estabelecimentos de estruturas de segurança, softwares preventivos como antivírus e antispywares nos ambientes de desenvolvimento de P&DI. Mas não apenas a proteção lógica deve ser considerada. O caso Snowden é um exemplo de que o elemento humano tem um potencial de acesso a sistemas que não pode ser descartado, pelo contrário, não pode deixar de haver proteções contra os chamados ataques físicos, ou seja, em que alguém, presencialmente, acessa a sistemas computacionais.

Martins e Santos (2005) destacam que no aspecto segurança física, áreas críticas como servidores só devem ser acessadas por pessoas autorizadas e, ainda assim, sob controle de entrada e saída, tanto de pessoas quanto de equipamentos. Recomendando-se a criação de normatizações de controles internos referente ao assunto, os quais devem sofrer auditoria periodicamente. Ainda assim, tratando-se de confidencialidade, a seleção adequada de pessoal é fundamental.

Outros dois ataques cibernéticos que chamam a atenção devido a falhas humanas, corrompendo a confidencialidade, são destacados por Singer e Friedman (2014). O primeiro caso citado pelos autores remota ao ano de 2008, quando um soldado dos EUA que passava por um estacionamento fora de uma base militar norte-americana no Oriente Médio encontrou um pendrive. Esse soldado inseriu o achado em um computador que estava conectado à rede militar de Comando Central americana e desencadeou uma das maiores brechas cibernéticas da história militar dos EUA, conhecida como Buckshot Yankee. Essa falha levou ao escaneamento de computadores da rede militar, a abertura de diversas portas de saída de dados e levou cerca de quatorze meses para ser sanada completamente pelo Pentágono.

O segundo caso destacado por Singer e Fiedman (2014) foi o de um executivo de uma companhia de Tecnologia da Informação que encontrou um CD que continha malware no banheiro masculino e resolveu verificar o conteúdo do referido disco. Desavisadamente, o executivo compartilhou projetos da aviônica do helicóptero presidencial norte-americano com hackers iranianos.

1.4 ATAQUES CIBERNÉTICOS CONTRA A INTEGRIDADE

A perda de integridade ocorre com a modificação ou destruição de informações de forma não autorizada. Ataques contra a integridade ocorrem, em geral, como atividade meio, não como um fim. Ao modificar algum dado, o atacante, normalmente, busca inserir backdoors para coletar informações, ou ainda, modificar a configuração de sistemas de automação para danificar ou obter controle das máquinas por eles controladas, entre outros.

1.5 ATAQUES CIBERNÉTICOS CONTRA A DISPONIBILIDADE

Machado et al. (2016) afirmam que a disponibilidade visa garantir o acesso sempre que necessário. Ou seja, o ataque cibernético contra a disponibilidade ocorre quando impossibilita o acesso a um sistema de informação, o uso de dados nele contido ou o torna inoperante. O uso crescente de automatização de sistemas é notório em diversas áreas, como indústrias, usinas de geração de energia, sistemas de vigilância e monitoramento remoto, entre outros. Nesses setores, a inoperância dos sistemas controladores pode indisponibilizar linhas de produção, câmeras de vigilância e até motores turbinas responsáveis por geração elétrica. Muitos desses sistemas controladores são informatizados, ou seja, passíveis de sofrer ataques cibernéticos, de procedência interna e externa.

Ataques cibernéticos contra sistemas controladores de processos produtivos já ocorreram. Um caso conhecido é o Stuxnet, em que um malware foi utilizado para atuar sobre os computadores que controlavam centrífugas de uma usina de enriquecimento de urânio, tornando o processo produtivo dessa usina inoperante.

Setores como o comércio, o de serviços, como o financeiro e de telecomunicações são alvos de ataques cibernéticos e estão passíveis de sofrer elevadas perdas se seus computadores ou servidores tornarem-se indisponíveis.

Finalmente, setores relacionados à gestão de mobilidade como o controle de trafego aéreo, trânsito e linhas férreas são exemplos de áreas em que ataques cibernéticos causadores de indisponibilidade são capazes de criar transtornos de elevadas magnitudes, tanto para os cidadãos comuns, quanto para empresas e governos, afetando, direta ou indiretamente, a economia da área atacadas.

2 ATAQUES CIBERNÉTICOS: DIMENSÕES ECONÔMICAS

Tratar economicamente aspectos relacionados a ataques cibernéticos não é tarefa trivial. Os prejuízos causados por possíveis danos a sistemas computacionais são facilmen-

te perceptíveis, no entanto, sua quantificação não é banal e apresenta elevados níveis de complexidade. Não obstante, há estudiosos que têm enfrentado esse desafio.

Hale (2002) afirma que os crimes cibernéticos no mundo atingiam, aproximadamente, a quantia de US$ 50 bilhões em 2002. Lewis (2018) destaca que, dentre os crimes praticados globalmente, os cibernéticos estão em terceiro lugar em geração de custos, atrás da corrupção nos governos e do narcotráfico. Ele adiciona que as estimativas existentes dos custos dos crimes cibernéticos apresentam variações significativas, indo de US$ 10 bilhões a mais de US$ 1 trilhão, o que reflete a baixa confiabilidade nos dados e nas diferentes metodologias de cálculo. Lewis (2018), por exemplo, utilizou a metodologia economic history research, chegando à estimativa de custo global dos crimes cibernéticos de até US$ 600 bilhões.

A dificuldade de obtenção de dados precisos e que representativos é exposta por CEA (2018) que afirma que houve elevada relutância das empresas em relatar informações negativas. Isso é reforçado por Scott (2016) que aponta apenas 13,2% dos crimes cibernéticos ocorridos no Reino Unido como reportados às autoridades policiais ou ao Action Fraud, que é o órgão britânico ao qual são informadas atuações criminosas dessa natureza.

Assim, Cashell et al. (2004) concluem que modelos teóricos que descrevem os retornos dos gastos em segurança da informação fornecem alguma ideia sobre o tamanho das perdas potenciais, mas a ausência de dados estatísticos melhores faz com que a determinação, de modo geral, dos custos dos ataques cibernéticos continue sendo especulativa. Essa percepção é coerente com a posição de CEA (2018) que afirma que as estatísticas divulgadas podem apresentar posições tendenciosas em razão dos dados obtidos.

CEA (2018) destaca que apesar de, normalmente, não divulgarem as perdas sofridas por ataques cibernéticos, as empresas ofertantes de seguros são as que provavelmente possuem as melhores condições de avaliar em que níveis essas perdas encontram-se, uma vez que ressarcem a seus clientes quando sofrem tais danos. Isso certamente é considerado pelas seguradoras para avaliar os riscos aos quais seus clientes estão expostos e quanto deve cobrar pelos seus seguros contra danos causados por ataques cibernéticos.

Essas dificuldades de estimativas fornecem o panorama em que se insere a caracterização das consequências econômicas de ataques cibernéticos. Muitas vezes, analistas dessa problemática precisam basear-se em considerações qualitativas sobre diferentes tipos de ataques cibernéticos identificados e sobre casos práticos ocorridos em variados setores ao redor do mundo.

Apesar dos números difusos, é notório que os ataques cibernéticos apresentam crescimento significativo, o que pode ser inferido pelo aumento progressivo das estimativas como, por exemplo, dos ataques de ransomware que, segundo Microsoft (2016), somaram US$ 325 milhões em 2015. Adicionalmente, Morgan (2017a) estima que esse valor foi de, aproximadamente, US$ 1 bilhão em 2016 e com previsão de cerca de 5 bilhões em 2017.

Tal cenário é tão preocupante que os riscos de ataques cibernéticos figuram entre os 10 maiores riscos de colapsos globais de 2018, do Fórum Econômico Mundial (WEF, sigla em inglês), classificado em terceiro em probabilidade de ocorrência e em sexto em termos de impactos (WEF, 2018).

O Fórum Econômico Mundial coloca os ataques cibernéticos atrás apenas de eventos climáticos extremos e desastres da natureza, no critério de análise probabilidade. Quando se consideram os impactos gerados, ficam abaixo dos dois anteriores somados a armas de destruição em massa, fracasso na adaptação às mudanças climáticas e crises relacionadas à água. Assim, os ataques cibernéticos foram entendidos como causadores de impactos maiores do que relevantes ameaças como

conflitos entre Estados, ataques terroristas, desemprego e crises relacionadas à fome.

Esses elevados impactos são ratificados por Morgan (2017b) quando destaca que há previsão de que os crimes cibernéticos gerem um custo mundial acima de US$ 6 trilhões anuais em 2021, o que representaria o dobro de 2015.

Com tais níveis de relevância, surge a indagação: como ocorrem tantos incidentes cibernéticos? Uma resposta parcial é que muitos tipos de ataques estão diretamente relacionados à procedimentos inadequados dos usuários, como os caso já mencionados do soldado norte-americano no Oriente Médio e do executivo que inseriu um CD de procedência desconhecida em sua máquina. Contudo, a maior parte dos ataques é iniciada por meio de links enviados às vítimas. Sobre esse aspecto, Zetter (2015) estima que 91% dos ataques sofisticados são iniciados por phishing ou spear phishing enviados por e-mail. Obviamente, se o usuário clicar nos links desconhecidos recebidos por correio eletrônico, ele estará contribuindo para o aumento da vulnerabilidade da rede a que participa.

Como resposta ao aumento das ameaças, as instituições passaram a investir cada vez mais em medidas preventivas, como contratação de prestadores de serviços de segurança cibernética e treinamento de funcionários. A respeito disso, Mello Júnior (2017) estima que esse treinamento preventivo dos colaboradores pode criar um mercado que gira em torno de US$ 10 bilhões em 2027.

Do exposto, torna-se evidente que os ataques cibernéticos oferecem iminente ameaça a setores produtivos, financeiros e até a segurança nacional de países. Por essa razão, diversos Estados criaram ou estão em processo de criação de mecanismos para fortalecerem suas capacidades de defesa nesse campo.

3 COMBATE E PREVENÇÃO AOS ATAQUES CIBERNÉTICOS

3.1 CONCEITOS RELACIONADOS À SEGURANÇA E DEFESA CIBERNÉTICA

Sabendo das possibilidades criadas e o quão danoso pode ser o advento cibernético, os países passaram a buscar soluções para prevenirem-se de possíveis ataques nos níveis

governamentais, ou ainda, para desenvolverem capacidades ofensivas, caso necessário, em um cenário denominado Guerra Cibernética. Da mesma forma, o setor privado busca proteger-se dos ataques cibernéticos, tendo em vista que é o principal alvo dos criminosos em tempos de paz.

O advento do espaço cibernético criou o conceito de segurança cibernética que "é a arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas" (BRASIL, 2014a, p. 19).

Outro conceito surgido foi o de defesa cibernética que, para Oliveira et al. (2017, p. 13), é o "ato de defender o sistema crítico das TIC de um Estado. Além disso, ela engloba as estruturas e questões cibernéticas que podem afetar a sobrevivência de um país". Já para o MD, esse é um conceito mais restrito, assim definido:

> Defesa cibernética é o conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente. (BRASIL, 2014a, p. 18)

O conceito de proteção cibernética é, para o MD, uma atividade de caráter permanente que abrange ações para neutralizar ataques e exploração cibernética contra os dispositivos computacionais e redes de computadores e de comunicações (BRASIL, 2014a, p. 23). Esse último conceito é o que melhor se adequa aos setores da iniciativa privada, o que não significa que lhe é exclusivo, uma vez que todos devem buscar fazê-lo. Por fim, o conceito de Guerra Cibernética que é, em resumo, o uso do espaço cibernético em operações militares.

3.2 SEGURANÇA E DEFESA CIBERNÉTICA PELO MUNDO

A União Internacional de Telecomunicações (ITU) publicou o Índice Global de Segurança Cibernética (GCI, sigla em inglês) 2017. Esse índice é considera 25 parâmetros que compõem 5 pilares: legal, técnico, organizacional, capacitação e cooperação (ITU, 2017).

Analisando o GCI é possível verificar os distintos níveis dos países em relação à temática cibernética. O Brasil aparece na 38ª posição, com índice 0,59338, figurando como o quinto das Américas, atrás de EUA, Canadá, México e Uruguai. Nessa análise, o Brasil foi classificado pela ITU como "em fase de amadurecimento".

Há distintos modelos para tratar de segurança cibernética e defesa cibernética. Segundo Oliveira et al. (2017), há basicamente três deles, com uma pequena variação no terceiro modelo. O primeiro, adotado por países como EUA, Colômbia e Venezuela, utiliza estruturas militares como responsáveis tanto pela defesa quanto pela segurança cibernética. O segundo, adotado no Paraguai, utiliza estruturas civis que também tratam incidentes cibernéticos na esfera militar. E o terceiro modelo é o adotado por países como Brasil e Argentina, que possuem estruturas civis para lidar com a segurança cibernética e estruturas militares para a defesa cibernética. Por fim, há uma variação do último modelo, adotada pelo Uruguai. Nele existem estruturas distintas bem definidas para os setores civil e militar, que são responsáveis, respectivamente, pela segurança e pela defesa cibernética. Contudo, a Política de Defesa uruguaia prevê a atuação das estruturas militares de defesa cibernética também no setor privado.

Os crimes cibernéticos são tratados como relevante à segurança nacional por diversos governos. Os EUA, por meio da Divisão Cibernética do FBI, investigam casos de invasão de computadores, contraterrorismo e contrainteligência como as principais prioridades do programa cibernético devido à sua possível

relação com a segurança nacional (FBI, 2018). Segundo FBI (2018), foi criada, recentemente, uma força-tarefa composta por diversas agências do governo, dentre elas o Departamento de Defesa, o Departamento de Segurança Interna e o próprio FBI, com o objetivo de trabalharem em conjunto para combater os crimes cibernéticos.

Algo semelhante ocorre na Austrália, onde, segundo Office of Prime Minister (2017), o governo investiu US$ 230 milhões na Estratégia Nacional Segurança Cibernética em 2016 e o Livro Branco de Defesa da Austrália prevê incremento de até US$ 400 milhões para melhoria das capacidades de defesa cibernética do país.

Na Europa, segundo o National Cyber Security Centre (NCSC), a União Europeia (UE) reconheceu que qualquer incidente de segurança cibernética poderia afetar vários Estados-Membros e, em 2013, apresentou uma proposta para melhorar a sua preparação para ataques cibernéticos. Essa proposta tornou-se, em 2016, uma diretiva denominada The EU Directive on the security of Network and Information Systems, dando aos Estados-Membros 21 meses para integrarem a diretiva nas respetivas legislações nacionais (NCSC, 2018).

O Reino Unido, segundo o UK Cabinet Office (2016) elevou o orçamento em defesa cibernética de £ 860 milhões para £ 1,9 bilhões, entre 2016 e 2021, com ênfase em três áreas: defesa de estruturas críticas nacionais como energia e transporte; retaliação a atacantes; e formação de uma geração de especialistas, com ênfase no investimentos em centros de pesquisa e ensino de segurança cibernética nas escolas.

Segundo o NCSC (2018), serão implementadas mudanças na legislação do Reino Unido, conforme a Diretiva de Segurança de Redes e Sistemas de Informação da UE, visando aumentar os níveis de segurança e resiliência globais dos sistemas de rede e de informação, obtendo, assim, base jurídica para dispor de um quadro nacional para gerir incidentes de segurança cibernética e criar um grupo de cooperação com os membros da UE para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações, participando de uma rede de para promover uma cooperação operacional em incidentes específicos de segurança de redes e sistemas de informação, bem como partilhar informações sobre os riscos. (NCSC, 2018)

Hakmeh (2017) afirma que nos países do Conselho de Cooperação do Golfo (GCC, sigla em inglês) há significativa diferença da forma com que os países membros tratam legalmente os crimes cibernéticos. A autora põe como fundamental haver aspectos legais definidos nas legislações dos países para que o combate aos crimes cibernéticos seja efetivo, como a definição de leis sobre o tema, tipificação criminal, regulação de interação entre Estados com fins cooperativos, definição de poderes processuais, definição de termos e os parâmetros de sua aplicação, estabelecimento de regras para provas eletrônicas, definição de sua jurisdição e a descrição da responsabilidade dos prestadores de serviços.

Todos os países do Conselho de Cooperação do Golfo possuem leis sobre crimes cibernéticos, porém, segundo Hakmer (2017), essas, em sua maioria, apenas concentram-se na criminalização.

Hakmer (2017) enfatiza que a melhor forma de combater os crimes cibernéticos é a cooperação internacional, sem a qual, a efetiva atuação tende a ser ineficiente, pois as técnicas operativas dos atacantes mudam com elevada velocidade. Assim, a autora destaca que é necessário haver compartilhamento de informações, inteligência, experiências e lições aprendidas para encontrar as melhores maneiras de conter o crime cibernético e abordar seus desafios, para tanto, ferramentas regulatórias, legais e tecnológicas precisam ser desenvolvidas coletivamente e atualizadas continuamente.

Dessa forma, verifica-se que o tema

da defesa cibernética consta da pauta governamental nas diversas regiões do mundo.

4 PASSADO PRESENTE E FUTURO DE ATAQUES CIBERNÉTICOS NO BRASIL

4.1 PASSADO

Desde 2006, o Brasil rompeu a barreira de mais de 100 mil incidentes cibernéticos reportados ao CERT.br em um ano. Desde então, apresentou uma forte tendência de crescimento desse número, com um pico em 2014, com mais de 1 milhão de incidentes reportados (CERT.br, 2018b). Esses números são menores do que os reais, pois nem todos os incidentes são reportados. Entretanto, ainda assim, permitem a obtenção de um panorama geral.

O Brasil é um alvo relevante de ataques cibernéticos. A esse respeito, há estudos que indicam o destaque para os ataques com finalidade de obtenção de vantagens financeiras. Lewis (2018), em sua análise para a Mcafee, identificou o impacto econômico de crimes cibernéticos em países como Austrália, Brasil, Canadá, Alemanha, Japão, México, Reino Unido e Emirados Árabes Unidos. Nesse estudo, Lewis (2018) aponta o Brasil como um dos novos centros de crimes cibernéticos, juntamente com a Índia, Coreia do Norte e Vietnã.

Lewis (2018) classifica o Brasil em segundo lugar no número de ataques cibernéticos originados no território e o terceiro principal alvo. Assim, o autor aponta que as leis brandas poderiam ser uma das causas de que 54% dos ataques cibernéticos reportados no Brasil são originários de dentro do próprio país, tendo como principal alvo, os bancos e instituições financeiras. Esse dado é coerente com os apresentados pelo CERT.br (2018c) em que 51,77% dos ataques que lhe foram reportados procederam do Brasil.

No Brasil existem leis que tratam sobre o tema, como a Lei nº 12.737, de 30 de novembro de 2012, conhecida popularmente como Lei Carolina Dieckmann, que dispõe sobre a tipificação criminal de delitos informáticos, alterando o Código Penal Brasileiro (BRASIL, 2012a) e a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, conhecida como Marco Civil da Internet (BRASIL, 2014b). Assim, é possível que tais leis sejam ineficazes para inibir a criminalidade pois na primeira lei, as penas não ultrapassam três anos de prisão e a segunda não contempla penalidades aos infratores.

O cenário descrito de leis brandas, associado à possibilidade de ganhos elevados com os cibernéticos e percepção de impunidade, cria uma relação de custo-benefício para os criminosos em que incentiva a realização de ataques.

A atuação governamental no sentido de fortalecer as capacidades de proteção cibernética para o país pode, indiretamente, contribuir para a redução da falha de mercado criada pelos ataques cibernéticos, se forem criadas medidas que incentivem ações conjuntas entre os setores públicos e privados. Uma vez que os conhecimentos necessários para proteger instalações críticas, como hidrelétricas apresentam semelhanças aos de proteger outros tipos de instituições, seria viável a atuação conjunta. Tal parceria contribuiria tanto para reduzir as falhas de mercado, quanto para fortalecer a defesa nacional que, por definição, é um bem público.

Em virtude de aspectos como os mencionados, a atuação do Estado é importante e desejável. Assim, medidas foram tomadas para adequar o Brasil ao cenário enfrentado. Ao criar a Política Nacional de Defesa em 2008, com revisão em 2012, o Brasil classificou o setor cibernético, juntamente com o nuclear e o espacial como estratégicos (BRASIL, 2012b). Isso permitiu a inclusão do setor cibernético na Estratégia Nacional de Defesa (END) o que, segundo Brasil (2014a), permitiu que a Segurança Cibernética e a Defesa Cibernética passassem a ser reconhecidas como campos sob responsabilidade de atuação do Estado.

Em 2009, segundo Brasil (2018a), o MD designou o EB como responsável pelo estabelecimento do setor cibernético, criando-se o Projeto de Defesa Cibernética. Esse ganhou proporções maiores, sendo substituído pelo Programa Estratégico do Exército Defesa Cibernética em 2016. Moury (2017) complementa que a prioridade do Governo Brasileiro com a defesa e a proteção cibernética levaram ao surgimento do Comando de Defesa Cibernética (ComDCiber) em 2016. Esse comando passou a funcionar com pessoal das três Forças Armadas, além de especialistas civis.

A END apresentou entre seus objetivos: promover ações conjuntas entre os Ministérios da Defesa e da Ciência, Tecnologia e Inovação contemplando o incentivo à multidisciplinaridade e dualidade de aplicações, fomento da Base Industrial de Defesa, aquisição de conhecimentos, geração de emprego e proteção das infraestruturas estratégicas do Brasil (BRASIL, 2012b). Esse contexto permitiu a estruturação do Estado Brasileiro na formatação adotada em 2018.

4.2 PRESENTE

No Brasil, atualmente, a responsabilidade de proteger os ativos nacionais no espaço cibernético são divididas para os setores civil e militar. Tal divisão ocorre de acordo com nível de atuação dos agentes públicos.

Segundo Brasil (2017a), a responsabilidade do planejamento, coordenação e desenvolvimento de ações de segurança cibernética é do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI-PR). Já a defesa cibernética age no nível estratégico. Assim, o DSIC/GSI-PR é encarregado pelo nível político; o ComDCiber pelo estratégico; o Centro de Defesa Cibernética pelo operacional e unidades militares das forças componentes pelo nível tático.

Alguns objetivos da END já ocorrem, como a aquisição de conhecimentos, produzindo o desenvolvimento de ferramentas com aplicação dual na área de cibernética. Pode-se citar o Simulador de Operações de Guerra Cibernética (SIMOC) que é um simulador virtual que foi desenvolvido com tecnologia 100% nacional, pelo EB em parceria com uma empresa de TIC. O SIMOC destina-se ao treinamento e simulação de situações para as tropas contra possíveis ataques cibernéticos (BRASIL, 2018b).

Na busca pelo fortalecimento das capacidades de defesa cibernética, o Governo Brasileiro trabalha conjuntamente com organizações públicas e privadas. Por exemplo, em 2018, ocorreu o primeiro exercício de simulação de ataques em massa aos setores financeiro, nuclear e de defesa, utilizando o SIMOC em Brasília. Esse exercício conjunto contou com a participação de gestores de crise e técnicos da área de proteção cibernética de instituições do setor financeiro, como Banco Central, bancos, empresas do setor nuclear, Ministérios da Defesa, das Relações Exteriores, Presidência da República e entidades do setor cibernético (BRASIL, 2018b).

Outro exemplo de parceria visando aumentar a resiliência aos ataques cibernéticos foi o acordo assinado entre a Fundação Parque Tecnológico Itaipu (FPTI) e o EB em 2017, esse acordo trata sobre cooperação mútua no Laboratório de Segurança Eletrônica, de Comunicações e Cibernética que funciona desde 2015 no Complexo Hidrelétrico de Itaipu (BRASIL, 2017b).

A colaboração entre agentes externos é necessária para o crescimento mútuo. Dessa forma, há atividades conjuntas com países que mantêm relações com o Brasil com o objetivo de trocar conhecimentos, um exemplo é o Estágio Internacional de Defesa Cibernética conduzido pelo EB, havendo a participação de representantes de vários países (BRASIL, 2018c).

Por fim, ainda sobre as parcerias internacionais, segundo (ITU, 2017), a Polícia Federal do Brasil participa do sistema global de comunicações policiais I-24/7 desenvolvido

pela Interpol para conectar policiais, incluindo crimes cibernéticos.

4.3 FUTURO

Percebe-se a tendência de crescimento do uso do espaço cibernético tanto por cidadãos quanto por criminosos. Esse cenário, leva ao entendimento de que novas ações visando combater aos crimes cibernéticos deverão ser executadas, tanto pelo setor privado como pelo governo.

Os órgãos governamentais responsáveis pela defesa cibernética e pela segurança cibernética tendem a crescer de importância no país. Esse crescimento pode criar externalidades positivas como o fortalecimento das capacidades de reação e mesmo prevenção de ataques a diversos setores. Para tanto, faz-se necessário a criação de políticas públicas para permitir que haja maior atuação conjunta de órgãos como o CERT.br, polícias especializadas e Forças Armadas, de preferência, com a participação de órgãos de proteção ligados a setores estratégicos do país.

Como há carência de leis específicas tratando sobre ataques cibernéticos, prospecta-se que essa deve ser uma pauta a ser discutida pelos legisladores. Por exemplo, Martins (2018) destaca que ainda não há legislação específica sobre proteção de dados no Brasil e que dois anteprojetos de lei estão em discussão no Congresso Nacional.

CONCLUSÃO

O presente trabalho estudou os ataques cibernéticos tratando sobre seus riscos, como são tratados por governos ao redor do mundo e no Brasil.

Conclui-se que o uso do espaço cibernético se encontra em plena expansão e que Governos de diversas regiões estão a tomar medidas que proporcionem interação entre a defesa e proteção cibernética de Estado com elementos da iniciativa privada. Assim, o modo de proteger um sistema governamental ou de infraestruturas críticas para um país pode robustecer os sistemas empresariais e vice-versa. Dessa forma, o Brasil começa a caminhar nessa direção com a aproximação de órgãos do governo, Forças Armadas e instituições públicas e privadas.

Por fim, conclui-se que o tema apresenta amplo espaço para estudos futuros, sendo afeto a vários campos do conhecimento.

CYBER ATTACKS AND GOVERNMENT ACTIONS TO COMBAT THEM.

ABSTRACT: The use of cyberspace grows every day. The cyber attacks have accompanied this growth whith constant threat. These attacks compromise the confidentiality, integrity and/or availability of data, systems and services, with negative reflections upon varied sectors of the economy. The objective of this article is to study the cyber attacks, their risks and those being treated by governments around the world and in Brazil. Data from secondary sources were used. It was identified that Brazil is in the intermediate level of cybersecurity, according to the criteria of the International Telecommunication Union. It was identified that the majority of cyber attacks suffered in Brazil reported to CERT.br originate from inside the country, which may be a consequence of the lack of specific laws to eliminate the impunity of offenders. It was found that a process of approximation between government agencies and the private sector has started to collaborate in the improvement of cybernetic protection capacity in Brazil.

Key words: Cyber attacks, Brazil, Defense.

REFERÊNCIAS

BRASIL. Casa Civil. Lei nº 12.737, de 30 de novembro de 2012. Brasília: 2012a.

_____. Ministério da Defesa. Política Nacional de Defesa e Estratégia Nacional de Defesa. Brasília: 2012b. Disponível em: <https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em: 14 set. 2018.

_____. Ministério da Defesa. Doutrina Militar de Defesa Cibernética. Brasília: 2014a.

_____. Casa Civil. Lei nº 12.965, de 23 de abril de 2014. Brasília: 2014b.

_____. Casa Civil. Decreto Presidencial nº 9.031, de 12

de abril de 2017. Brasília: 2017a.

_____. Exército Brasileiro. Exército e Itaipu assinam acordo para incremento da segurança de estrutura estratégica vital para o país. Noticiário do Exército. Brasília: 5 set. 2017b. Disponível em: <http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/exercito-e-itaipu-assinam-acordo-para-incremento-da-seguranca-de-estrutura-estrategica-vital-para-o-pais->. Acesso em: 14 set. 2018.

_____. Escritório de Projetos do Exército Brasileiro. Coordena e integra a Defesa Cibernética. Brasília: 2018a. Disponível em: <http://www.epex.eb.mil.br/index.php/defesa-cibernetica/defesa-cibernetica>. Acesso em: 14 set. 2018.

_____. Exército Brasileiro. Exercício Guardião Cibernético reúne especialistas em TI, gestores de crise e tomadores de decisão. Noticiário do Exército. Brasília: 4 jul. 2018b. Disponível em: <http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/exercicio-guardiao-cibernetico-reune-especialistas-em-ti-gestores-de-crise-e-tomadores-de-decisao->. Acesso em: 14 set. 2018.

_____. Exército Brasileiro. Cooperação internacional e defesa cibernética atuam juntos para o enfrentamento das ameaças dessa natureza. Noticiário do Exército. Brasília: 14 mai. 2018c. Disponível em: <http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/cooperacao-internacional-e-defesa-cibernetica-atuam-juntos-para-enfrentamento-das-ameacas-dessa-natureza->. Acesso em: 14 set. 2018.

CALDAS, Daniel Mendes. Análise e extração de características estruturais e comportamentais para perfis de malware. Dissertação. UnB: Brasília, 2016. Disponível em: <http://repositorio.unb.br/handle/10482/23110>. Acesso em: 23 out. 2017.

CARVALHO, Paulo Sergio Melo de. A defesa cibernética e as infraestruturas críticas nacionais. Coleção Meira Mattos – Revista das Ciências Militares. Rio de Janeiro, 2011.

CASHELL, Brian; JACKSON, William D.; JICKLING, Mark e WEBEL, Baird. The Economic Impact of Cyber-Attacks. Government and Finance Division. Congressional Research Service. The Library of Congress. 1th Apr, 2004. n. RL32331. Disponível em: <https://fas.org/sgp/crs/misc/RL32331.pdf>. Acesso em: 12 set. 2017.

CEA (THE COUNCIL OF ECONOMIC ADVISERS). The Cost of Malicious Cyber Activity to th U.S Economy. Washington, Feb, 2018. Disponível em: <https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>. Acesso em: 18 jul. 2018.

CEBROWSKI, A. K. Transformation and the Changing Character of War? Transformation Trends, Office of Transformation, Department of Defense. Arlington, 17 Jun. 2004. Disponível em: <www.hsdl.org/?view&did=448180>. Acesso em: 14 out. 2017.

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). Cartilha de Segurança para Internet: ransomware. 25 mai. 2018a. Disponível em: <https://cartilha.cert.br/ransomware/>. Acesso em: 8 set. 2018.

_____. Total de incidentes reportados ao CERT.br por ano. 2018b. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 12 set. 2018.

_____. Incidentes reportados ao CERT.br – Janeiro a Dezembro de 2017. 2018c. Disponível em: <https://www.cert.br/stats/incidentes/2017-jan-dec/top-cc.html>. Acesso em: 14 set. 2018.

EASTTOM, William Chuck. Computer Security Fundamentals. Pearson IT Certification, 3 ed. 2016.

FEDERAL BUREAU OF INVESTIGATION (FBI). What we investigate: Cyber Crime. U.S. Government, U.S. Departament of Justice. 2018. Disponível em: <https://www.fbi.gov/investigate/cyber>. Acesso em: 2 jul. 2018.

GASPAR, Philipe. Pragas eletrônicas: ainda não estamos livres delas. jul. 2007. Disponível em: <http://www.philipe.eti.br/artigo-003.pdf>. Acesso em: 22 out. 2017.

HAKMER, Joyce. Cybercrime and the Digital Economy in the GCC Countries. Chatham House. The Royal Institute of International Affairs. International Security Departmente. London: Jun. 2017. Disponível em: <https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf>. Acesso em: 16 set. 2018.

HALE, Chris. Cybercrime: Facts & Figures Concerning This Global Dilemma. Crime & Justice International. v. 18, Issue 65, p. 5, 6, 24-26, Sep. 2002. Disponível em: <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=197384>. Acesso em: 30 jan. 2018.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). Global Cybersecurity Index 2017. Genebra: 2017. ISBN: 978-92-61-25071-3. Disponível em: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf>. Acesso em: 27 set. 2018.

KLIMBURG, Alexander. National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn, 2012.

LEWIS, James. Economic Impact of Cybercrime – No Slowing Down. Mcafee Report – CSIS. Santa Clara, CA, February. 2018. Disponível em: <https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email>. Acesso em: 31 jul. 2018.

MACHADO, T. G.; MOTA, A. A.; MOTA, L. T. M.; CARVALHO, M. F. H. e PEZZUTO, C. C. Methodology For the Cybersecurity Maturity Level Identification in Smart Grids. IEEE Latin America Transactions. v. 14, issue 11, p. 4512-4519, Nov. 2016. Disponível em: <http://www.revistaieeela.pea.usp.br/issues/vol14issue11Nov.2016/14TLA11_14GerardMachado.pdf>. Acesso em: 22 jan. 2018. DOI: 10.1109/TLA.2016.7795822

MARTINS, Alaíde Barbosa; SANTOS, Celso Alberto Saibel. Uma metodologia para implantação de um Sistema de Gestão de Segurança da Informação. JISTEM: Journal of Information Systems and Technology Management, vol. 2, n. 2, 2005, pp. 121-136. ISSN online: 1807-1775. Universidade de São Paulo. São Paulo. Disponível em: <http://www.redalyc.org/pdf/2032/203219587002.pdf>. Acesso em: 22 jan. 2018.

MARTINS, Danylo. Invasões cibernéticas criminosas ameaçam os negócios. Valor Econômico. Finanças. São Paulo: 28 mai. 2018. Disponível em: <https://www.valor.com.br/financas/5552593/invasoes-ciberneticas-criminosas-ameacam-os-negocios>. Acesso em: 5 out. 2018.

MELLO JÚNIOR, John P. Security Awareness Training Explosion. Cybersecurity Ventures. Menlo Park, California: 6 Feb. 2017. Disponível em: <https://cybersecurityventures.com/security-awareness-training-report/>. Acesso em: 8 set. 2018.

MICROSOFT. Helthcare Beware the Rise of Ransomware. 31 May. 2016. Disponível em: <https://cloudblogs.microsoft.com/industry-blog/industry/microsoft-in-business/healthcare-beware-the-rise-of-ransomware/>. Acesso em: 8. set. 2018.

MORGAN, Steve. Global Ransomware Damage Costs Predicted to Exceed $ 5 Billion in 2017. Cybersecurity Ventures. Menlo Park, California: 18 May. 2017a. Disponível em: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. Acesso em: 8 set. 2018.

_____. Cybercrime Damages $ 6 Trillion By 2021. Cybersecurity Ventures. Menlo Park, California: 16 Oct. 2017b. Disponível em: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. Acesso em: 8 set. 2018.

MOURY. Taciana. Exército Brasileiro investe em defesa cibernética. Diálogo: Revista militar digital – Fórum das Américas. 12 mai. 2017. Disponível em: <https://dialogo-americas.com/pt/articles/brazilian-army-invests-cyber-defense>. Acesso em: 14 set. 2018.

NATIONAL CYBER SECURITY CENTRE (NCSC). Introduction to the NIS Directive. London: 28 Jan. 2018. Disponível em: <https://www.ncsc.gov.uk/guidance/introduction-nis-directive>. Acesso em: 16 set. 2018.

OFFICE OF PRIME MINISTER. Offensive Cyber Capability to Fight Cyber Criminals. Media release. Austrália: 30 Jun. 2017. Disponível em: <https://www.pm.gov.au/media/offensive-cyber-capability-fight-cyber-criminals>. Acesso em: 14 ago. 2018.

OLIVEIRA, Marcos A. G.; PAGLIARI, Graciete D. C.; MARQUES, Adriana A.; PORTELA, Lucas S. e FERREIRA NETO, W. B. Guia de Defesa Cibernética na América do Sul. Recife: Ed. UFPE, 2017.

OPPERMANN, Daniel. Governança da internet e segurança cibernética no Brasil. Monções: Revista de Relações Internacionais da UFGD. Dourados, v.2, n.3, jul./dez., 2013.

PAIS, Ricardo; MOREIRA, Fernando; VARAJÃO, João. Engenharia Social (ou o carneiro que afinal era um lobo). Universidade de Minho – Portugal. Ed. Almedina, p. 171–187, 2013. Disponível em: <http://hdl.handle.net/1822/26251>. Acesso em: 4 nov. 2017.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 7, n. 58, 1 ago. 2002. Disponível em: <https://jus.com.br/artigos/3186>. Acesso em: 21 out. 2017.

RAPOSO, Álisson Campos. Terrorismo e contraterrorismo: desafio do século XXI. Revista Brasileira de Inteligência/Agência Brasileira de Inteligência. vol. 3, n. 4, set, p. 39–55. Brasília, 2007.

SIKORSKI, Michael e HONIG, Andrew. Practical Malware Analysis. No Starch Press. San Francisco, 2012.

SINGER, Peter Warren; FRIEDMAN, Allan. Cybersecurity and cyberwar: what everyone needs to know. 2014.

Segurança e Guerra cibernéticas: o que todos precisam saber. Tradutor Geraldo Alves Portilho Junior. Rio de Janeiro: Biblioteca do Exército Editora, 2017.

SCOTT, Patrick. How much of a problem is cyber-crime in the UK? The Telegraph. United Kingdom, 1th Nov. 2016. Disponível em: <https://www.telegraph.co.uk/news/2016/11/01/how-much-of-a-problem-is-cyber-crime-in-the-uk/>. Acesso em: 7 ago. 2018.

UK CABINET OFFICE. Britain's cyber security bolstered by world-class strategy. United Kingdom: Nov. 2016. Disponível em: <https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy>. Acesso em: 14 ago. 2018.

VENTRE, Daniel. Ciberguerra. In: ACADEMIA GENERAL MILITAR. Seguridad global y potencias emergentes en un mundo multipolar. XIX Curso Internacional de Defensa. España: Universidad Zaragoza. p. 31-45, 2011. Disponível em: <https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF48.pdf>. Acesso em: 1 set. 2018.

VIANNA, Eduardo Wallier; FERNANDES, Jorge Henrique Cabral. O gestor da segurança da informação no espaço cibernético governamental: grandes desafios, novos perfis e procedimentos. Brazilian Journal of Information Science: Research Trends, v. 9, n. 1, Marília, 2015. DOI 10.22556/1981-1640.

WORLD ECONOMIC FORUM (WEF). The Global Risks Report 2018, 13th Edition. Geneva: 2018. ISBN: 978-1-944835-15-6. Disponível em: <http://www3.weforum.org/docs/WEF_GRR18_Report.pdf>. Acesso em: 15 ago. 2018.

ZETTER, Kim. Hacker Lexicon: what is phishing? Wired. EUA: 4 jul. 2015. Disponível em: <https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/>. Acesso em 8 set. 2018.

Washington Rodrigues da Silva é instrutor na Escola de Comunicações do Exército Brasileiro (EsCom) é mestre em Economia da Defesa na Universidade de Brasília (UnB). Graduado em Administração pela Faculdade de Ciências da Administração da Universidade de Pernambuco (FCAP/UPE) (2010) e em Ciências Militares pela Academia Militar das Agulhas Negras na área de Comunicações (AMAN) (2004). Especialista em Administração Financeira pela Faculdade de Ciências da Administração da Universidade de Pernambuco (2010), em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO) (2012), Gestão de Sistemas Táticos de Comando e Controle pela EsCom (2014) e Guerra Eletrônica pelo Centro de Instrução de Guerra Eletrônica (CIGE) (2015). Atua na área de Defesa e Educação no Exército Brasileiro. Foi instrutor do Centro de Preparação de Oficiais da Reserva do Recife (CPOR/R) (2007 a 2011); compôs a equipe de instrução da EsCom (2013 a 2015) e foi instrutor na Escuela de Comunicaciones da Escuela de las Armas do Exército Argentino (EcCom/EDA) (2016). Pode ser contatado pelo e-mail washingtonrs@hotmail.com.

Jorge Madeira Nogueira é Professor Titular do Departamento de Economia da Universidade de Brasília (ECO/UnB). Formado em Economia pela Universidade Federal do Rio de Janeiro (1975), Jorge Madeira Nogueira obteve seu título de Mestre em Engenharia de Produção pela Coordenação dos Programas de Pós-graduação em Engenharia da Universidade Federal do Rio de Janeiro (1978), com doutorado em Desenvolvimento Agrário - University of London (1982) e Pós-doutorado em Economia Regional pela Cornell University, Estados Unidos (1992). Ingressou como professor no Departamento de Economia da Universidade de Brasília (ECO/UnB) em 1983. Entre 1991 e 1995 foi Professor Visitante na Universidade de Cornell nos Estados Unidos. Em Cornell, ele recebeu o BURNHAM KELLY AWARD FOR DISTINGUISHED TEACHING - Prêmio concedido ao melhor professor do ano, eleito por alunos e professores, do College of Planning. Sua produção acadêmica inclui pouco mais de 150 trabalhos publicados em periódicos ou em anais de congressos científicos. Jorge Madeira Nogueira foi membro do Conselho Consultivo do Fundo Vale para o Desenvolvimento Sustentável entre 2013 e 2017. Pode ser contatado pelo e-mail jmn0702@unb.br.

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

EDUCAÇÃO

REPOTENCIALIZAÇÃO COGNITIVA DA ARMA DE COMUNICAÇÕES

Ricardo Inacio Dondoni
Pós-graduado em Ciências Militares

RESUMO: A Arma de Comunicações ocupou-se da difícil tarefa de mesclar o ensino técnico e tático em consonância com os avanços tecnológicos promovidos no material que apoia seu emprego. Para o estabelecimento das bases da Arma, mesclou-se ensino promovido pela Academia Militar das Agulhas Negras (AMAN), Escola de Comunicações e Instituto Militar de Engenharia, consolidando as expertises dessas escolas na gênese do militar de comunicações. Com a solidificação dos conhecimentos no Curso de Comunicações, a formação vinculou-se às Escolas de Formação (AMAN e ESA). Os intensos avanços científicos nas décadas posteriores promoveram emprego de faixas de frequência pouco estudadas e o surgimento de tecnologias, hoje, indispensáveis, cujo ensino não era objeto da antiga formação. O presente artigo identifica carências cognitivas na formação dos militares de Comunicações que podem ser suplantadas por reformulação curricular ou pela promoção de módulos de ensino a distância. Para isso, foi formulada uma pesquisa e enviada a 32 organizações militares de comunicações e respondida por 220 militares. O universo da seleção foi representado por militares envolvidos na atividade finalística, administrativa e de ensino. Os resultados apontaram para a necessidade de atualizações em três áreas: basilares, como por exemplo, matemática, física, antenas e propagação; estratégicas, como por exemplo, predição de enlace em HF com ênfase no emprego de ionossondas; e de interesse tecnológico, que permitem o uso de tecnologia proveniente da linha de fronteira do conhecimento.

Palavras-chave: Ensino. Atualização Curricular. Comunicações.

INTRODUÇÃO

A história remonta à 1ª Guerra Mundial (1914-18) como o evento no qual a necessidade das comunicações superou quaisquer expectativas, por mais promissoras que essas fossem.

A nova realidade, onde os campos de batalha eram mais amplos e complexos, demandava sinergia e encadeamento de ações rápidas e precisas (HISTORIA, [198-?]).

Nesse contexto, surgia as Comunicações como uma arma de apoio ao combate[1].

No Brasil, a criação da Escola de Comunicações, em 1º de julho de 1921, marcou o nascimento da Arma do Comando.

O núcleo de preparação de especialistas em comunicações permaneceu instalado na 2ª Companhia do 1º Batalhão de Engenharia por dois anos, passando a funcionar, a posteriori, na Escola de Aperfeiçoamento de Oficiais até, enfim, ocupar sede própria em Deodoro.

Os eventos da 2ª Guerra Mundial (1939-45) firmaram inabalavelmente a imprescindibilidade das Comunicações diante do

> alargamento dos campos de batalha, a utilização dos meios de combate e armas cada vez mais sofisticadas e mortíferas, e ainda, a dispersão imposta as operações, que agravaram a necessidade crescente e imperiosa dos comandos de manterem em suas mãos o controle absoluto das ações. (HISTORIA, [198-?])

Já não era mais possível almejar êxito sem o eficiente domínio e eficaz emprego dos meios de comunicações. Por assim dizer:

> Isto acabou por colocar as comunicações no campo daquelas armas imprescindíveis ao combate e sem as quais nenhuma vitória sequer pode ser imaginada. (HISTORIA, [198-?])

A gênese da arma de Comunicações incluiu em seus primórdios, militares formados pela Academia Militar das Agulhas Negras

1. A Arma de apoio ao combate complementa a missão das armas-base (Infantaria e Cavalaria), quer pelo apoio de fogos, quer pela mobilidade e contramobilidade ou, ainda, pela instalação e manutenção de toda a infraestrutura necessária ao exercício do Comando e [...] Controle.

(AMAN); oficiais subalternos possuidores do curso de Oficial de Comunicações, ministrado pela Escola de Comunicações; oficiais engenheiros de comunicações do quadro técnico da ativa (hoje extinto) e, ainda, os oficiais da arma de Engenharia, possuidores do Curso de Oficial de Comunicações (HISTORIA, [198-?]).

Nos primeiros anos de existência, por disposição da Lei nº 3.654, de 4 de novembro de 1959, por força do Art 25:

> O oficial subalterno de comunicações será chamado, com toda a sua turma de formação da Academia Militar das Agulhas Negras, para fazer o curso de engenheiros de comunicações, no Instituto Militar de Engenharia. (BRASIL, 1959)

Pela gênese embrionária a qual foi submetido, o comunicante deveria ser a perfeita amálgama entre o técnico e o tático, capaz de compreender o complexo mundo das ciências exatas com seu viés tecnológico, produzindo eficiente apoio às necessidades operacionais e táticas.

Essa característica peculiar da arma proporcionou conhecimento sólido na confecção dos manuais técnicos, onde é possível verificar a apresentação dos resultados de estudos científicos sem, no entanto, a exposição complexa e exaustiva dos cálculos que os antecedem. Dessa forma, transliterou-se as complexas equações em leitura inteligível aos militares formados em outras especificidades.

A consolidação da formação do Oficial de Comunicações na Academia Militar, acarretou no emprego dinâmico do formando nos corpos de tropa, como ocorria com todas as demais armas, quadro e serviço. O Oficial de Comunicações da AMAN já não era mais chamado a fazer o curso de engenheiros de comunicações no IME, sendo formado unicamente pela AMAN.

A inexistência de estudos complementares no IME pouco afetariam as primeiras turmas formadas, haja vista os inexpressivos avanços científicos ocorridos até meados de 1973. Assim sendo, os conhecimentos adquiridos pelas turmas formadas na AMAN e IME seriam replicados sem perdas significativas durante longo período.

Em 1973, com o advento da telefonia celular, o mundo começa a experimentar um recrudescimento nas inovações científicas, muitas delas ligadas às telecomunicações.

Passados 27 anos, os primeiros aparelhos celulares começaram a ser comercializados no Brasil. A partir daí, os avanços foram contínuos e ininterruptos.

A tecnologia celular sofreu saltos significativos entre suas gerações (1G, 2G, 3G, 4G e 4.5G, estando a tecnologia às portas daquilo que caracterizará o 5G). A internet, antes discada, passou a ser oferecida em banda larga via cabo, fibra ótica, wi-fi e enlace satelital. Faixas de frequências eletromagnéticas inexploradas passaram a ser empregadas. Iniciaram-se estudos em formatos de onda não-ortogonais em busca de “estruturas de transmissor e receptor ótimos e sub-ótimos, na modelagem e análise matemática dos sistemas incluindo o canal” (ARAÚJO, 2012), com significantes resultados na eficácia do emprego, a saber, maior aproveitamento da faixa e menor interferências no espectro.

Para cada avanço supracitado, houve uma linha de pesquisa exaustivamente trabalhada, resultados publicados e dados confrontados. E, como consequência, a linha do conhecimento científico foi ultrapassada sucessivas vezes desde 1973, gerando informação nova e necessária ao pleno aproveitamento dos recursos de telecomunicações empregados pela Força Terrestre e que consubstanciam o soldado do futuro.

O presente estudo visa levantar, de forma embrionária, as carências cognitivas que possam limitar o exercício pleno das capacidades esperadas aos integrantes da Arma de Comunicações. Também propõe um alinhamento cognitivo, no viés tecnológico, junto ao processo de transformação da Força Terrestre, objetivando minimizar o hiato tecnológico e científico criado pelos sucessivos avanços do

conhecimento científico na área das telecomunicações e afins.

1.1 TRANSFORMAÇÃO DA FORÇA TERRESTRE

Apesar do artigo limitar-se a apresentar carências cognitivas afetas à arma de Comunicações, essas esteiam, de forma embrionária e útil, uma análise da arma, segundo o processo de transformação do Exército, que busca capacitá-lo a atuar frente

> a imprevisibilidade e a incerteza do ambiente internacional, as indicações dos cenários prospectivos – onde se visualiza uma crescente demanda por alimentos, recursos hídricos, energéticos e minerais – as novas tecnologias presentes no mundo atual e em constante evolução, as mudanças no ambiente operacional – cada vez mais urbano e sofrendo a interferência de novos atores internacionais, governamentais e não governamentais – e as profundas mudanças nos processos de atuação das forças militares são indutores para transformação dos atuais meios militares. (O PROCESSO, 2010)

O projeto Transformação do Exército se reveste de abrangência superior, mas é possível perceber nele a mesma tônica presente neste artigo: identificar a realidade atual e preparar-se para as necessidades vindouras.

O projeto estrutura-se em sete vetores que, consoantes, apontam para a visão de futuro, em prol da "construção de um novo instrumento de defesa terrestre, mais efetivo e adequado a essa nova realidade" (O PROCESSO, 2010). São eles:

a) 1º Vetor - Doutrina

b) 2º Vetor - Preparo e Emprego

c) 3º Vetor - Educação e Cultura

d) 4º Vetor - Gestão de Recursos Humanos

e) 5º Vetor - Gestão Corrente e Estratégica

f) 6º Vetor - C&T e Modernização do Material

g) 7º Vetor - Logística

A apresentação vetorizada dos tópicos estruturantes do projeto cumpre o papel dinâmico de promover avanços graduais, sistemáticos e concomitantes, viabilizando a consecução dos objetivos intermediários, bem como o acompanhamento das fases e retificação dos processos, quando necessário.

Todos os vetores se interrelacionam e, portanto, avanços no vetor de C&T e Modernização do Material promoverão ações no vetor de Preparo e Emprego, bem como no vetor de Educação e Cultura. Assim sendo, a título de exemplificação, quaisquer aquisições de equipamentos, dotados de tecnologias oriundas da fronteira do conhecimento, acarretarão em desenvolvimento de ações nos quesitos relacionados à educação, capacitação e inovação.

Desse viés surge a urgência em identificar capacidades desejadas e nível de cognição onde são ensinadas para formular uma proposta de atualização de currículos escolares nos estabelecimentos de formação ou, ainda, criar módulos de nivelamento de conhecimentos em plataformas de ensino a distância, identificando a trilha do conhecimento pertinente a cada universo da seleção.

2 METODOLOGIA

Trata-se de um estudo exploratório, que levou em consideração apenas as necessidades técnicas da formação dos militares da arma de Comunicações. Necessidades, explicitamente táticas, não fizeram parte da presente abordagem. No entanto, permanecem relevantes para estudos posteriores.

Com o objetivo de identificar os aspectos cognitivos deficitários na formação atual, foram coletados dados provenientes de disciplinas de cursos ofertados aos oficiais integrantes do Forte Marechal Rondon no período de 2015 a 2017.

Dentro do período supracitado, inden-

tificam-se duas vertentes básicas, a saber, atender às necessidades de capacitação de pessoal aos militares vinculados ao Sistema de Monitoramento de Fronteiras e promover capacitação de instrutores de estabelecimentos de ensino instalados no Forte, concomitantemente com a atualização de currículos escolares desses estabelecimentos.

Das propostas de trabalho vigentes à época, destaca-se aquela apresentada pelo Instituto Nacional de Telecomunicações (INATEL), cuja síntese era alcançar os objetivo propostos pela execução de duas fases distintas, a saber, o nivelamento dos participantes e o aprofundamento dos assuntos de interesse.

O presente artigo levou em consideração o conteúdo programático a que foram submetidos, os óbices cognitivos que promoveram o nivelamento, bem como o trabalho realizado em conjunto por ambos estabelecimentos de ensino (EsCom e CIGE), na identificação de conteúdo programático que promovesse nivelamento de comunicações aos integrantes da Força Terrestre.

A síntese resultou no espectro de disciplina e conhecimentos elencados no Quadro 1:

QUADRO 1 Ementa das disciplinas e conteúdos programáticos

DISCIPLINA	CONTEÚDO PROGRAMÁTICO
Nivelamento em Sistemas de Comunicações	visão geral dos principais sistemas de comunicações e visão geral do diagrama de bloco de um transceptor
Nivelamento em Técnicas de Transmissão	multiplexação FDM, TDM, CDM, OFDM e múltiplo acesso, espalhamento espectral, MIMO
Nivelamento em Propagação	modos de propagação (´terrestre, troposférico e ionosférico'), parâmetros notáveis ´refratividade, permissividade do solo, condutividade, raio de curvatura da terra, estudo da atmosfera da terra, atenuação pela chuva, gases´, enlace em visibilidade, zonas de fresnel, propagação em obstáculos gume de faca, planejamento de enlace rádio, módulos de propagação aplicados a ferramentas de simulação, aspectos e usos das faixas de frequência ´HF, VHF, UHF, SHF´
Nivelamento em Modulação Analógica e Digital	conceitos básicos de banda base e banda passante, linhas de transmissão em banda base e suas aplicações, conceitos de interferência interssimbólica, diagrama de olho, BER, MER, SNR, CNR, eficiência espectral, eficiência de energia, desempenho e robustez de modulações, modulações analógicas, amplitude, frequência e fase, modulações de banda passante, ruído de canal, ruído térmico, conceito de intermodulação passiva e seus efeitos na comunicação, conceitos de desvanecimento, tipos de desvanecimento e seus efeitos na comunicação e processamento digitais de sinais
Nivelamento em Sinais Analógicos	processamento, formato, processos de amostragem, quantização e codificação
Nivelamento em Antenas	conceitos de antenas, campo próximo, distante e suas implicações, parâmetros das antenas ´Banda passante, polarização, diagrama de irradiação, impedância, diretividade, área de efeito, relação frente-costas´, tipos de antenas e sistemas em que são empregadas ´vertical, microstrip, dipolo, parabólicas, guia de onda fendido, cornetas, helicoidais, yagi-uda, log-periódica, discone, antenas encurtadas com capacitadores e indutores´, arranjo de antenas ´PhasedArray, interpretação de parâmetros de datasheet de antenas, sistemas de recepção com amplificador'
Cálculos de Decibeis	Cálculo de ganho em decibéis de tensão e potência
Interferências	interferências eletromagnéticas e filtros contra interferências eletromagnéticas
Resistividade e Condutividade	resistividade elétrica e condutividade elétrica
Predição de Enlace em HF	Camadas da ionosfera, MUF, FOT, LUF, equador magnético, ionossondas e cálculos de predição.
Nivelamento em Codificação de Fonte e Decanal	Nivelamento em codificação de fonte e decanal (teoria da codificação, taxa e ganho de codificação, principais códigos)
Tecnologia Celular	Principais características das gerações de telefonia 1G, 2G, 3G e 4G, tecnologias de acesso múltiplo e formas de duplexação; arquiteturas LTE/SAE, IMS e PCC; princípios das técnicas OFDM; protocolos e interfaces na rede de acesso; protocolos e interfaces no núcleo de rede; principais procedimentos, bearers, features para a release
Nivelamento em Equipamentos de Instrumentação	Instrumentos de medição 'multímetro, osciloscópio, analisador de espectro, wattímetro, analisador de rede vetorial´, linhas de transmissão e analisador de redes, medição de impedância de cabos coxiais, medição de faixa de frequência de operação de antenas

DISCIPLINA	CONTEÚDO PROGRAMÁTICO
Nivelamento em Tecnologia da Informação	infraestrutura, desenvolvimento, segurança e implantação de cultura de segurança da informação e comunicação
Nivelamento em Matemática	logarítmo, trigonometria, matrizes, probabilidade e estatística, números complexos, vetores e fasor, transformada de sinais contínuos e discretos
Nivelamento em Física	unidades, relações e conversões de unidades, eletricidade e magnetismo, ótica e ondulatória
Nivelamento em Eletro-óptica	descrição geral dos sistemas de comunicações ópticas e aplicações, teoria da radiação infravermelha e teoria geral do laser
Nivelamento em Inglês Técnico	na área do conhecimento da Informática, Eletricidade, Telecomunicações e Informática

Fonte: o autor, 2018.

As disciplinas e conteúdos programáticos integraram a pesquisa, com perguntas na modalidade aberta e fechada, encaminhadas à 32 organizações militares de Comunicações. A pesquisa foi respondida por 220 militares, aleatoriamente distribuídos entre os universos de oficiais e praças, na faixa etária de 24 a 54 anos, todos oriundos de Comunicações, dos quais: 67% possuíam maior tempo de vivência profissional no exercício das atividades operacionais; 24% possuíam maior tempo de vivência profissional envolvido nas atividades administrativas; e 9% possuíam maior tempo de vivência profissional no exercício das atividades de ensino. A amostra possuía as seguintes características: Idade M=39+-15, sendo 77 oficiais e praças. Os dados foram coletados entre 5 e 29 de março de 2018.

Os indivíduos foram subdivididos em grupos etários da seguinte forma: Até 5 anos de vivência profissional englobando os 3º Sargentos, Aspirantes a Oficial, 2º Tenentes e 1º Tenentes; de 6 a 10 anos englobando 3º Sargentos mais antigos e Capitães; de 11 a 15 anos englobando 2º Sargentos, Capitães mais antigos e Majores recém promovidos; de 16 a 20 anos englobando Majores antigos e 1º Sargentos e, ainda, acima de 21 anos de serviço para Subtenentes, Tenentes do Quadro Auxiliar de Oficiais, Tenentes Coronéis e Coronéis. As faixas supracitadas não computaram os tempos de formação acadêmica.

3 RESULTADOS E DISCUSSÕES

Os resultados permitem maior percepção das carências cognitivas que afetam o exercício pleno das capacidades esperadas aos integrantes da Arma de Comunicações na instrução, nos exercícios militares ou, ainda, na aquisição de material. A limitação cognitiva é passível de afetar as três atividades nas quais comumente os comunicantes estão envolvidos.

3.1 O PROBLEMA DAS RELEVÂNCIAS COGNITIVAS

Um dos subprodutos da presente pesquisa foi o ordenamento de relevância dos nivelamentos cognitivos em consonância com os anseios dos militares de Comunicações, conforme exposto no QUADRO 2.

QUADRO 2 Prioridade de nivelamento segundo resultados da pesquisa

Prioridade	(% Absoluta)	(% Relativa)	DISCIPLINA
1	68,37 %	100 %	Nivelamento em Antenas
2	66,31 %	95,52 %	Nivelamento em Propagação
3	60,20 %	88,06 %	Nivelamento em Sistemas de Comunicações
4	57,65 %	84,33 %	Nivelamento em Tecnologia da Informação
5	53,06 %	77,61 %	Nivelamento em Equipamentos de Instrumentação
6	50,51 %	73,88%	Nivelamento em Modulação Analógica e Digital

Prioridade	(% Absoluta)	(% Relativa)	DISCIPLINA
7	50,51 %	73,88%	Nivelamento em Técnicas de Transmissão
8	48,98 %	71,64 %	Interferências
9	46,94 %	68,66 %	Tecnologia Celular
10	42,86 %	62,69 %	Cálculos de Decibéis
11	39,80 %	58,21 %	Nivelamento em Inglês Técnico
12	38,27 %	55,97 %	Predição de Enlace
13	35,71 %	52,24 %	Nivelamento em Sinais Analógicos
14	32,65 %	47,76 %	Nivelamento em Física
15	30,10 %	44,03 %	Resistividade e Condutividade Elétrica
16	27,55 %	40,30 %	Nivelamento em Eletro-óptica
17	25,51 %	37,31 %	Nivelamento em Matemática
18	25,51 %	37,31 %	Nivelamento em Codificação de Fonte e Decanal

Fonte: o autor, 2018.
Legenda:

Crítico (100% - 85%) Alto (84% - 70%) Médio (69% - 55%) Baixo (54% - 40%) Planejável (39% - 25%)

Os resultados da coluna % Absoluta apresentam as porcentagens em consonância com o universo total da pesquisa, caracterizam a heterogeneidade dos dados e evidenciam a inexistência de quesitos de indicação unânime.

Os resultados da coluna % Relativa apresentam as porcentagens em consonância com o teto das indicações do quesito melhor votado, facilitando a mensuração da relevância entre os quesitos e, por conseguinte, tornando-se útil à apresentação dos resultados e promoção das discussões.

É mister destacar que o ordenamento acima apresenta itens que se complementam e interrelacionam, mas que foram priorizados em grau de importância distintos, posicionando-se nos extremos classificados. Essas discrepâncias revelam indícios de perda de cognição, inicialmente percebida de forma lenta e gradual; e intensificada pelos avanços científicos dos últimos 46 anos.

É fácil perceber que os assuntos identificados como de menor relevância formam a base conceitual necessária à promoção do conhecimento aos assuntos mensurados como de grande relevância. Sem a base conceitual não há livre pensamento. A implementação do nivelamento cognitivo busca diminuir o hiato conceitual crescente em razão nos avanços tecnológicos e implementação de novas tecnologias de informação e comunicação (TIC).

Por exemplo, os níveis cognitivos necessários ao desenvolvimento de um nivelamento em antenas faz expressivo uso de conceitos, teorias e fórmulas explicitadas nos nivelamentos de matemática e física, demonstrando não somente o relacionamento entre as partes, mas também, a imprescindibilidade desses nivelamentos para a promoção daquele. A ausência desses conhecimentos pode acarretar em prejuízo real nas instruções, operações e aquisição de material. Sem a cognição desejada, o instrutor é incapaz de promover a capacitação de pessoal. Sem as bases conceituais solidificadas, o discente é incapaz de promover, por si só, novas soluções para problemas antigos. Sem a absorção dos conceitos, os operadores do sistemas de telecomunicações ficam limitados a meras repetições de processos, incapazes de promover soluções adequadas a situações anômalas, sendo, portanto, ineficazes quando mais imprescindíveis se tornam. Sem o correto entendimento lógico e conceitual, pouco se percebe das reais características dos equipamentos a serem adquiridos, possibilidades de uso e limitações de emprego. A perda cognitiva nos assuntos basilares pode promover compras inadequadas de equipamentos, que levem em consideração

o merchandise promovido pela vendedora ao invés de identificar a aquisição que detém patentes em nível de estado da arte ou, ainda, de interesse da Força.

3.2 PERCEPÇÕES PONTUAIS

Uma vez apresentada a relevância dos tópicos em consonância com o total do universo pesquisado, a Tabela 1 identifica a distorção da relevância em conformidade com as faixas etárias apresentadas na metodologia.

As colunas apresentam os dados levantados para cada categoria. Esses dados estão implicitamente divididos por 5 faixas etárias (até 5 anos, de 6 a 10 anos, de 11 a 15 anos, de 16 a 20 anos e acima de 21 anos).

A primeira linha apresenta o valor médio resultante das faixas etárias.

A segunda linha apresenta a variância resultante da aplicação da fórmula abaixo:

$$\text{Variância} = \frac{\sum f_i.(X_i - \mu)^2}{n} \quad (1)$$

E a última linha apresenta o Desvio Padrão que é a raiz quadrada da variância.

Um baixo desvio padrão indica que os dados sob análise agrupam-se próximos ao valor médio. Valores altos indicam dados afastados do valor médio.

TABELA 1 Distorção de relevância da implementação de nivelamento cognitivo segundo faixa etária

Prior da Tabela 1	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII
Geral	Nvl Antenas	Nvl Propagação	Nvl Sis Com	Nvl TI	Nvl Instrumentação	Nvl Tec Tx	Nvl Mod Analog e Dig	Interferências	4G e 5G	Cálculo de dB	Nvl Inglês Técnico	Predição de Enlace
Média	26,8	25,60	23,60	22,60	20,80	19,80	19,80	19,20	18,40	16,80	15,60	15,00
Variância	172,80	135,20	69,20	159,20	102,80	94,80	52,80	122,80	73,20	54,80	123,20	154,00
Desvio Padrão	13,15	11,63	8,32	12,62	10,14	9,74	7,27	11,08	8,56	7,40	11,10	12,41

Fonte: o autor, 2018.

Os nivelamentos em Antenas, Tecnologia da Informação, Predição de Enlace, Inglês Técnico, Propagação, Interferências Eletromagnéticas e Instrumentação apresentaram maior grau de desvio padrão, indicando que, além dos aspectos mensurados no QUADRO 1, as classes etárias apresentam percepções distintas das necessidades cognitivas relacionadas ao tema afeto, conforme pode ser visto na TABELA 1.

Os desvios padrões (DP) com valores altos resultam de uma amplitude de dados elevada. Os dados catalogados dentro das cinco faixas etárias apresentaram diferença acentuada com relação à média de valores do quesito em análise. Isso quer dizer que a percepção da necessidade do nivelamento não é comum a todas as faixas etárias. Os dados são heterogêneos, ou seja, existem faixas etárias que carecem de nivelamentos cognitivos específicos, enquanto outras não carecem. A tabela 1 destaca em vermelho os DP que mais caracterizam essas necessidades individuais.

Os altos valores de DP, quando analisados conjuntamento com as variâncias que lhe subsidiam, geram novos indicadores. Por exemplo, valores altos de variância nas faixas etárias mais baixas geram indícios de perda de conhecimento, enquanto que valores altos alocados nas faixas etárias mais altas geram indícios de ocorrência de melhorias no processo ensino-aprendizagem. Para fim de exemplificação, a Tabela 2 apresenta na prioridade IX o nivelamento em 4G e 5G, as gerações mais antigas denotam necessitar de nivelamento cognitivo, expresso pelo alto índice de variância, enquanto as gerações mais recentes não indicam como relevante um nivelamento nessa área do conhecimento, por possuírem óbices significativos em outras áreas.

Em todos os casos, os dados da tabela limitam-se a apresentar os cálculos em consonância com a veracidade da informação prestada na ocasião de sua coleta e, ainda, não são capazes de mensurar as razões de seleção de um quesito em detrimento de outro.

Sendo assim, os dados são uteis para identificar a percepção e servem de subsídios para novas aferições, que filtrem mais os resultados alcançados.

TABELA 2 Variâncias mensurados por faixas etárias

Prior da Tabela 1	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII
GERAL Variância	Nvl Antenas	Nvl Propa-gação	Nvl Sis Com	Nvl TI	Nvl Instru-mentação	Nvl Tec Tx	Nvl Mod Analog e Dig	Interferên-cias	4G e 5G	Cálculo de dB	Nvl Inglês Técnico	Predição de Enlace
5 A	23,04	21,16	0,16	0,36	0,64	14,44	14,44	27,04	5,76	33,64	1,96	100,00
6 - 10 A	10,24	40,96	5,76	29,16	0,64	27,04	4,84	4,84	1,96	0,04	54,76	49,00
11 - 15 A	77,44	43,56	43,56	31,36	33,64	23,04	14,44	10,24	5,76	0,64	6,76	1,00
16 - 20 A	10,24	0,36	0,36	43,56	0,64	3,24	1,44	3,24	1,96	10,24	57,76	4,00
21 - 30 A	51,84	29,16	19,36	54,76	67,24	27,04	17,64	77,44	57,76	10,24	1,96	0,00

Fonte: o autor, 2018.

A tabela 2 identifica as carências por faixa etária, possibilitando promover soluções setoriais que levem em consideração a relação custo x benefício.

Promover nivelamento a todas as faixas, concomitantemente, envolve abastados recursos orçamentários, ampla capacidade gerencial e dispendioso emprego de recursos humanos, o que dificulta promover uma solução que resolva todos os problemas instantaneamente. Sem contar que, para se identificar melhorias realizadas pelas ações empreendidas, é importante isolar uma variável por vez. Atuar em todas ao mesmo tempo poderá resolver o problema, mas impossibilitará a identificação da variável que promove o resultado.

Sugere-se considerar as prioridades elencadas na Tabela 1 em consonância com os óbices apresentados na Tabela 2, compartimentando as soluções segundo o interrelacionamento dos assuntos.

Apesar dos assuntos possuírem demasiado grau de relacionamento, é possível modularizar a transmissão do conhecimento e escalonar em trilhas de conhecimento. O Quadro 3 exemplifica a construção de módulos aos universos interessados, levando em consideração o interrelacionamento dos assuntos.

QUADRO 3 Exemplo de solução modular envolvendo antenas, propagação e cálculo de dB.

Assunto	Antena e Propagação		Cálculo de dB
Nível	Módulo I - Básico	Módulo II -Avançado	Módulo III - Complementar
Oficiais Superiores	X	X	-
Oficiais Intermediários	X	X	X
Oficiais Subalternos	X	X	X
Subtenentes	X	X	-
Sargentos	X	X	X
Cabos e Soldados	X	-	-

Fonte: o autor, 2018.

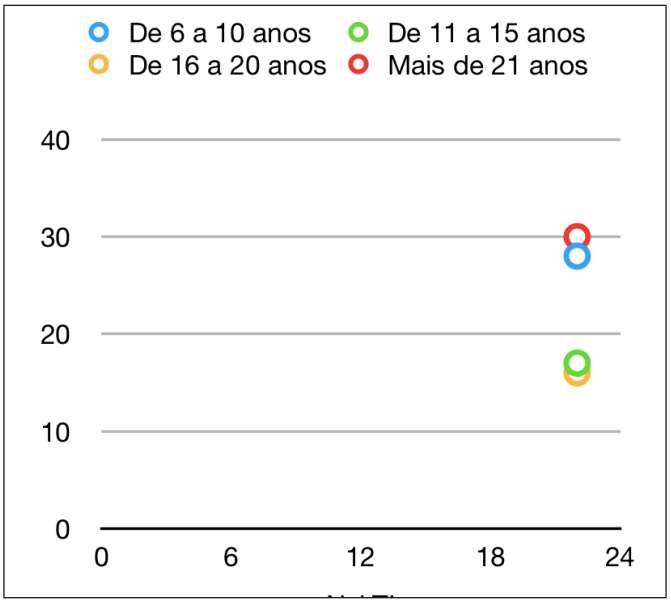
O Quadro 3 apresenta uma possibilidade de emprego dos dados componentes do Quadro 2, em consideração a relevância dos assuntos da Tabela 1, consubstanciado pelas informações presentes na Tabela 2. Outras possibilidades podem ser exploradas pela análise dos quadros e tabelas do presente artigo.

3.3 ANÁLISES SINGULARES

O Gráfico 1 apresenta os resultados da pesquisa quanto ao Nivelamento em Tecnologia da Informação. Os militares com menos de 20 anos de serviço fazem parte da geração que empregou equipamentos de TI desde a formação. É natural que esses militares julguem desnecessário um nivelamento nessa área, haja vista tratar-se de uma geração imersa na TI.

No entanto, percebe-se que os militares mais modernos acompanham o interesse nesse nivelamento. Entre as causas prováveis de interesse pela área, pode-se citar os avanços científicos no campo cibernético, envolvendo ataque, defesa e proteção cibernética. Nesse sentido, a geração mais moderna se iguala a mais antiga em necessidade de atualização cognitiva.

GRÁFICO 1 Interesse no nivelamento em TI



Fonte: o autor, 2018.

O Gráfico 2 apresenta os resultados da pesquisa quanto à predição de enlace. Enquanto três grupos apresentam resultados relativamente homogêneos, os militares mais modernos apontam para a carência cognitiva sobre o assunto. Neste ínterim, subsidiando a análise dos dados, alguns fatores devem ser levados em consideração, a saber:

a) os usuários mais conscientes quanto à necessidade de domínio sobre o tema são aqueles que fazem uso da faixa de frequência em HF, que foi pouco empregada nos eventos recentes;

b) a faixa de HF possui baixa capacidade de tráfego de dados e pouca pesquisa foi gerada com o objetivo de sanar essa lacuna, promovendo o emprego de outras faixas para explorar uma solução em transmissão de dados;

c) apenas recentemente, pesquisadores estão promovendo avanços tecnológicos significativos quanto ao emprego de dados em HF, como, por exemplo, verifica-se no caso do padrão Digital Radio Mondiale (DRM),

> "que possibilitaria comunicações multimídia acessíveis e seguras, de grande aplicação estratégica militar e civil" (OKAMURA, 2018);

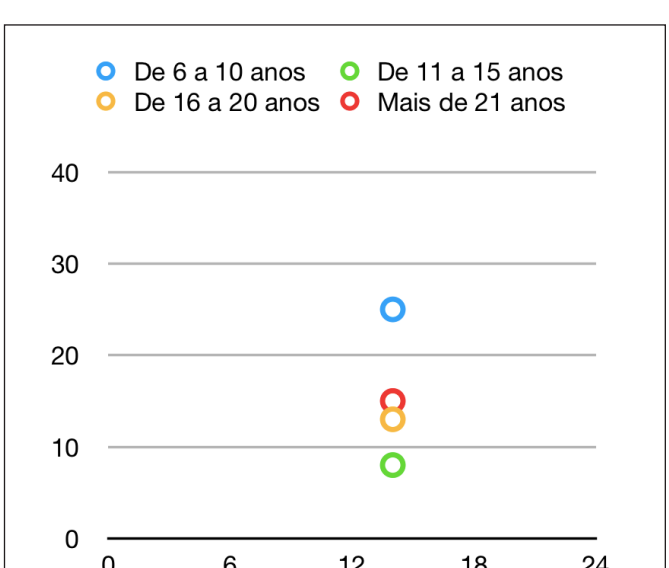
d) a solidificação dos conceitos de VPN concorreram para que o HF se tornasse um meio secundário para o estabelecimento de um enlace a distância;

e) a desinformação quanto ao uso das ionossondas para aquisição de dados precisos para o cálculo de enlace em HF gera descrédito no uso da faixa; e

f) o país encontra-se na zona do equador magnético, o que amplifica a dificuldade do uso da faixa de HF sem que sejam nivelados conhecimentos em predição de enlace.

Apesar do gráfico apontar carência cognitiva vinculada aos militares de formação recente, alguns avanços científicos, no uso do HF para transmissão de dados e emprego de ionossondas para estabelecimento da FOT, são inéditos até para as gerações menos carentes de conhecimento na área afeta.

GRÁFICO 2 Interesse no nivelamento em predição de enlace



Fonte: o autor, 2018.

Há de se levar em consideração que todos os fatores que dificultam o emprego da faixa tornam o emprego dela ainda mais relevante. Se o emprego é difícil para quem tem que trabalhar diariamente com ela, quiçá para uma eventual força oponente. O nivelamento de conhecimento em predição de enlace com ênfase na faixa de HF é primordial para os interesses do Estado e de extrema relevância para a Defesa Nacional.

CONCLUSÃO

O presente estudo levantou carências cognitivas passíveis de afetar o exercício das capacidades operacionais desejadas aos integrantes da Arma de Comunicações, ao mesmo tempo em que propõe o aprofundamento de estudos que vislumbrem a promoção de nivelamentos nas áreas citadas na pesquisa.

É imprescindível lembrar que nos idos da gênesis da arma, o comunicante era a perfeita amálgama entre o técnico e o tático, por força do decreto de criação e pelas gerações que se aproveitaram dos ecos cognitivos gerados pela dupla formação acadêmica inicial.

A atual geração está imersa em novas tecnologias e conceitos, que por sua vez, exploram faixas de frequências e modos de transmissão de informações, antes inexistentes, aproveitando pouco dos ecos cognitivos gerados por aquela formação.

Faz-se necessário um novo nivelamento cognitivo que permita, à arma de Comunicações, o domínio dos conceitos e tecnologias para promover a infraestrutura adequada às necessidades de Comando e Controle da Força Terrestre, em consonância com a visão de futuro proposta pelo processo de transformação do Exército.

Esse nivelamento, irremediavelmente, inicia-se pela promoção dos conceitos basilares em Matemática e Física, com aplicação no

campo da TIC, indo ao encontro das tecnologias de ponta, que sejam úteis e de interesse da Força Terrestre.

Além disso, o nivelamento deve repotencializar capacidades operacionais estratégicas como no caso da predição de enlace com ênfase no HF, além de fornecer subsídios a promoção de áreas de conhecimento de interesse da Força como no caso da cibernética.

No entanto, esses nem mesmo são os ganhos mais expressivos da proposição de um nivelamento cognitivo. É mister lembrar que o nivelamento tem capacidade de produzir reflexos na aquisição de materiais de emprego militar. Propõe-se com isso, não apenas a redução de custos de aquisição, mas também, orientar compras consonantes com a realidade de emprego militar. O sistema adquirido não deve estar aquém das necessidades, nem mesmo além das possibilidades de emprego.

A percepção cognitiva alcançada pelo nivelamento permite entender não apenas as limitações de cada sistema, mas também, identificar quem são os detentores das patentes tecnológicas de interesse da Força. Tal compreensão permite orientar as aquisições de forma a promover a interoperabilidade ne-

cessária ao bom funcionamento da Função de Combate Comando e Controle.

O estudo realizado apresenta aos orgãos decisores uma proposta de atualização na formação técnica dos militares da Arma de Comunicações, mesmo que em caráter embrionário.

Não foi objeto da pesquisa definir a forma de promoção dessa atualização cognitiva. Espera-se que estudos futuros julguem a eficácia da atualização dos currículos acadêmicos nas escolas de formação ou a difusão do conhecimento por meio de módulos de ensino a distância ou, ainda, a promoção de um período de dupla vigência até que uma seja suplantada pela outra.

COGNITIVE REPOTENCIALIZATION OF THE SIGNAL CORPS

ABSTRACT: The Signal Corps focused on the difficult task of merging technical and tactical education in line with the technological advances promoted in the material that supports its employment. For the establishment of the bases of the Signal Corps, a teaching promoted by the Academia Militar das Agulhas Negras (AMAN), Escola de Comunicações and Instituto Militar de Engeharia was merged, consolidating the expertises of these schools in the genesis of the military of communications. With the solidification of the knowledge in the Communications Course, the training was linked to the Training Schools (AMAN and ESA). The intense scientific advances in the following decades promoted employment of little studied frequency range, technologies unknown and the emergence of technologies, indispensable nowadays, whose education was not object of the old formation. This article identifies cognitive deficits in the training of military communications that can be supplanted by curricular reformulation or the promotion of distance learning modules. For this, a survey was formulated and sent to 32 military communications organizations and answered by 220 military personnel. The selection universe was represented by military personnel involved in the finalistic, administrative and teaching activity. The results pointed to the need for updates in three areas: basilar, such as mathematics, physics, antennas and propagation; such as, prediction of HF binding with emphasis on the use of ionosonde; of technological interest, that allow the use of technology coming from the frontier line of knowledge.

Keyword: Teaching. Curricular Update. Communications.

REFERÊNCIAS

ARAÚJO, D. C. Sistema de comunicações com sinais m-QAM não – ortogonais. 2012. 70 f. Dissertação (Mestrado em Teleinformática)-Centro de Tecnologia, Universidade Federal do Ceará, Fortaleza, 2012.

BRASIL. Lei nº 3.654, de 4 de novembro de 1959. Dispõe sobre a criação e organização do Quadro de Material Bélico, das Armas de Comunicações e de Engenharia, regula as condições de extinção do Quadro de Técnicos da Ativa e dá outras providências. **Diário Oficial da União** - Seção 1, 5 nov. 1959. Página 2336. Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/1950-1969/L3654.htm>. Acesso em: 18 dez. 2018.

HISTÓRIA da Arma de Comunicações. Rio de Janeiro: Curso de Comunicações da Academia Militar das Agulhas Negras, [198-?].

OKAMURA, Vitor Ossamu Rodrigues; ALVES, Plínio Ricardo Gamine. Uso estratégico de dados de ionossondas para comunicações digitais em alta frequência (HF). O Comunicante, [S.l.], v. 8, n. 3, p. 23-31, out. 2018. ISSN 2594-3952. Disponível em: <http://ebrevistas.eb.mil.br/index.php/OC/article/view/1794>. Acesso em: 09 jan. 2019.

O PROCESSO de Transformação do Exército. 3ª Edição. 2010. Disponível em: <http://www.eb.mil.br/c/document_library/get_file?uuid=18d47a84-99ac-45d3-b7d5-f37c9b5e53dc&groupId=1094704> Acesso em: 18 dez. 2018.

Ricardo Inacio Dondoni chefiou a Seção de Pós-graduação e Doutrina da Escola de Comunicações do Exército Brasileiro (EsCom) de 2016-18. É Graduado em Ciências Militares pela Academia Militar das Agulhas Negras na área de Comunicações (AMAN, 2002). Possui especialização em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO, 2011) e Psicopedagogia Clínica e Institucional pelo Instituto COTEMAR (2018)e pode ser contatado pelo e-mail dondoni.ricardo@eb.mil.br.

CONFERÊNCIA DE INICIAÇÃO CIENTÍFICA

em Assuntos de Defesa

CICAD.II.2018

DECEX

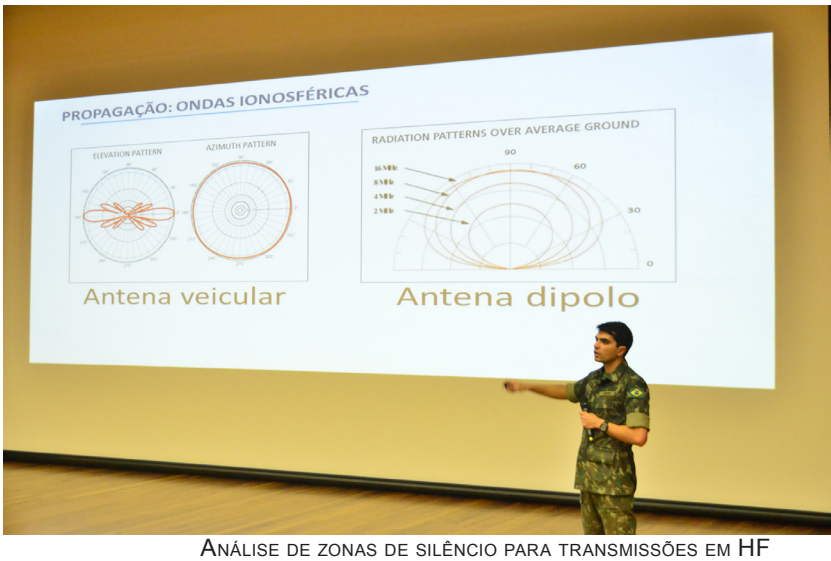
CCOMGEX

DCT

Recepção dos participantes da 2ª CICAD

Abertura da Conferência feita pelo Comandante da Escola de Comunicações, Cel Rodolfo Roque Salguero de La Vega Filho

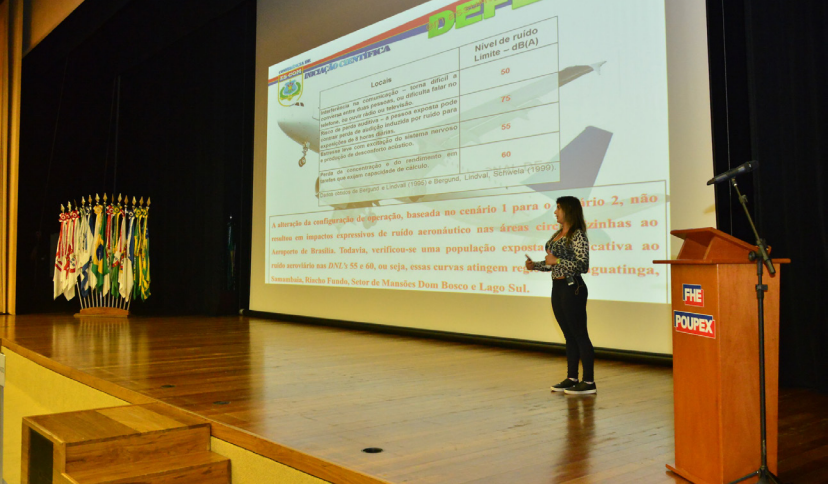
Implementação de testes de invasão em apoio à proteção cibernética de redes e sistemas de interesse da Defesa por Lucas Maurício Alves Zigunow



Análise de zonas de silêncio para transmissões em HF por Antonio Anderson Silva Marques

Composição da esquerda para a direita: Washington Rorigues da Silva, Victor Torres Kumm, Antônio Anderson Silva Marques

Palestrantes aguardando a formulação das perguntas



Avaliação do impacto do ruído aeronáutico no entorno de brasília por Raphaella de Souza Serapião Amorim

Cerimonialista da CICAD.II.2018

Eficácia de ataque cibernético do tipo spear phising por Victor Torres Kumm

Ataques Cibernéticos e Medidas Governamentais para Combatê-los por Washington Rodrigues da Siilva

Palestrantes aguardando a formulação das perguntas

Composição da esquerda para a direita: Lucas Maurício Alves Zigunow, Raphaella de Souza Serapião Amorim e Patrícia dos Reis de Morais

Endereço

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