ISSN 2594-3952

O Comunicante

SUMÁRIO

Artigos

Revista Científica da Escola de Comunicações

Escola Coronel Hygino Corsetti

VOLUME 8 - Nº 3

Outubro 2018

ISSN 2594-3952

O Comunicante

SUMÁRIO

Artigos

Revista Científica da Escola de Comunicações

Escola Coronel Hygino Corsetti

VOLUME 8 - Nº 3

Outubro 2018

EDITORIAL

O COMUNICANTE

Revista Científica da Escola de Comunicações

Ano 8 - Nº 3
Outubro 2018

ISSN 1968-6029
ISSN 2594-3952 (Digital)
Escola de Comunicações - EsCom
Escola Coronel Hygino Corsetti

O Comunicante - Revista Científica da Escola de Comunicações - Volume 8, Nº3(Out/2018)
Brasília-DF: Escola de Comunicações. 2018 88p; 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.

O COMUNICANTE

Revista Científica da Escola de Comunicações

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

Todos os textos submetidos devem vir acompanhados de carta de autorização para publicação que garantirá seu ineditismo ou, ainda, que apesar de 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.

EXPEDIENTE

EDITORIAL

A presente Edição da Revista “O Comunicante” reveste-se de caráter especial por apresentar os trabalhos científicos submetidos durante a 1ª Conferência de Iniciação Científica em Assuntos de Defesa (CICAD), conduzida por esta Escola no mês de junho de 2018. Os trabalhos contêm assuntos diversos, nas áreas de concentração das telecomunicações, tecnologia da informação, eletricidade e cibernética. Todos esses temas são relevantes para atividade de Defesa Nacional, mais especificamente sobre a atividade de Comando e Controle em operações militares.

Sobre o campo cibernético, especificamente, os trabalhos demonstram a importância do assunto no cenário atual. Segundo o General Robert Neller, Comandante do Corpo de Fuzileiros Navais dos Estados Unidos, o domínio do campo cibernético tornou-se o novo “centro de gravidade” na moderna estratégia militar. Assim, os artigos representam pequenas contribuições para o debate em torno da questão.

Destacam-se, ainda, a apresentação de artigos com temas de caráter transversal, como meio ambiente e educação a distância, sendo este último, uma das tendências que compõem o atual processo ensino-aprendizagem e evidenciam a necessidade de se buscar a capacitação continuada dos recursos humanos, valendo-se de novos métodos de ensino.

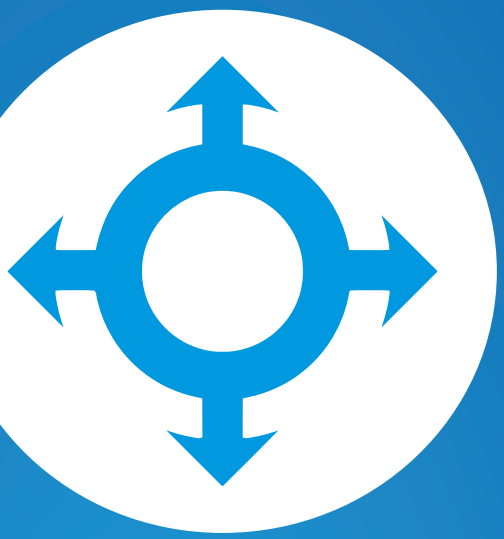
A participação crescente de contribuições de alunos e pesquisadores oriundos de instituições de ensino civis cumpre um dos objetivos propostos por esta publicação, estando alinhada com as diretrizes do sistema de educação e cultura do Exército Brasileiro e com a Estratégia Nacional de Defesa.

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

Desejamos a todos uma boa leitura.

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

Orientadores dos Artigos publicados



Anderson Gomes de Jesus

- Mestre em Ciência e Tecnologia Nucleares
- Coordenador Adjunto de Aperfeiçoamento Docente
- AMAN

http://lattes.cnpq.br/1866372877993798

Paulo Roberto Corrêa Leão

- Mestre em Gestão do Conhecimento e Tecnologia da Informação
- Coordenador dos Cursos de Pós-Graduação em Perícia Digital e Gestão de Projetos.
- UCB

http://lattes.cnpq.br/7110305735923934

Plínio Ricardo Ganime Alves

- Doutor em Engenharia Elétrica
- Professor associado 4 do Departamento de Engenharia Elétrica da Universidade de Brasília (UnB).
- UnB

http://lattes.cnpq.br/8921775057274048

CICAD.I.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

POSSÍVEIS EFEITOS DAS RADIAÇÕES NÃO IONIZANTES EM MILITARES DO EXÉRCITO BRASILEIRO

Gabriel Pascoal Zanateli Zappi Silva[1], Anderson Gomes de Jesus[2]
Graduado em Ciências Militares[1], Mestrado em Ciência e Tecnologia Nucleares[2]

RESUMO: Este trabalho trata de um breve estudo sobre os efeitos das radiações não ionizantes em militares do Exército Brasileiro, além de abordar os aspectos jurídicos da questão. A pesquisa conta com o levantamento de dados obtidos através de análises teóricas que serviram de base para o apontamento das características do espectro eletromagnético e verificação de seus possíveis efeitos, visando ao aprimoramento nas instruções dos Cadetes da Arma de Comunicações da AMAN e de tropas que operam os mais diversos meios de comunicações do Exército Brasileiro.

Palavras-chave: radiação não ionizante. efeitos biológicos. efeitos estocásticos.

INTRODUÇÃO

Atualmente, a questão sobre os efeitos biológicos das radiações não ionizantes tem adquirido importância, pois se trata de um conceito contemporâneo e requer a atualização do Exército Brasileiro (EB) nessa àrea do conhecimento, visto que os militares estão expostos aos mais diversos espectros de radiações, em especial, as radiofrequências, emitidas por equipamentos rádio nas operações.

Seu estudo é relevante para o meio militar, como forma de subsidiar as Organizações Militares de Saúde de informações por meio da análise dos efeitos das radiações não ionizantes nos combatentes.

Os militares que fazem uso de equipamentos rádio se submetem à exposição e correm o risco de sofrer os efeitos das radiações, em especial, os que pertencem à Arma de Comunicações, integradores da rede de uma Brigada em um Centro de Comunicações, que são expostos com maior frequência a uma gama de radiações.

O presente trabalho busca tratar do tema sob a perspectiva da verificação dos efeitos biológicos das radiações não ionizantes em militares. A abordagem tem como alicerce a tríade: tempo de exposição a radiações, intensidade dos campos eletromagnéticos e susceptibilidade quanto ao desenvolvimento de desordens físicas ou biológicas aos combatentes.

Delimita-se o foco investigativo na análise dos efeitos biológicos das radiações não ionizantes dos militares do EB expostos às radiofrequências emitidas pelos equipamentos em uso nas diversas unidades do Exército. A partir disso, a probabilidade de desenvolver complicações físicas ou biológicas de menor ou maior grau após um elevado tempo de exposição à radiação não ionizante será elucidada.

Nessa esteira, pretende-se verificar a relação entre radiação ionizante e não ionizante e evidenciar que por mais que não haja compensação orgânica a militares expostos a radiações não ionizantes, esta possui um grau de periculosidade que deve ser levado em consideração pelo responsável pelas operações nas diversas unidades.

Os objetivos específicos deste trabalho são: concluir, confirmando ou não, a hipótese do militar exposto às radiações não ionizantes sofrer algum de seus possíveis efeitos; e verificar os aspectos jurídicos da exposição laboral a campos elétricos e magnéticos.

1 METODOLOGIA

Com vistas a investigar as lacunas no conhecimento até agora existente é oportuno problematizar a questão: militares da Arma de Comunicações, que operam equipamentos

transmissores de radiofrequências já desenvolveram determinado efeito físico ou biológico durante ou após uma operação?

A falta de efetivos tecnicamente capacitados dificulta o revezamento para operar os equipamentos-rádio em uma operação. Além disso, sua conscientização não é feita pelo fato dos estudos das radiações não ionizantes serem recentes. A pesquisa desenvolvida está vinculada à premissa da possibilidade de os combatentes sofrerem algum efeito referente à radiação não ionizante ao operarem os diversos equipamentos que transmitem ondas no nível das radiofrequências.

Pode-se enunciar as hipóteses da seguinte maneira:

a) não há o devido esclarecimento dos operadores quanto ao espectro eletromagnético nos períodos em que passaram por instruções nos bancos escolares da AMAN/EsSA/EsLog;

b) os operadores de equipamentos, que emitem radiofrequências, desenvolveram algum sintoma após um período de permanência em um ambiente tal como um centro de comunicações que concentra as comunicações da Brigada.

Logo, as seguintes variáveis foram estudadas: existência de instruções nos bancos escolares aos militares em formação, que propiciasse o devido conhecimento acerca dos efeitos biológicos das radiações não ionizantes e, também, sobre os possíveis efeitos físicos ou térmicos em operadores de equipamentos na faixa das radiofrequências ou micro-ondas.

Visou-se especificamente à exposição da carência de conhecimento na fonte dos bancos escolares em relação ao ensino da temática supracitada. Fato esse que pode vir a criar um ambiente de trabalho que afete a qualidade de vida dos militares que sofrem incidência eletromagnética das naturezas em estudo.

Quanto à qualidade das fontes encontradas, destacam-se, pela qualidade, pertinência e atualidade, as pesquisas de Heinrich (2002) na definição de radiações eletromagnéticas e de Catalão (2010) que subdivide a radiação não ionizante em três grandes frentes, além de fazer definir precisamente o que é bioeletromagnetismo.

2 RESULTADOS E DISCUSSÕES

2.1 CONCEITOS BÁSICOS

2.1.1 Radiação não ionizante

De todas as regiões do espectro eletromagnético contidas na Tabela 1, as radiações não ionizantes são aquelas que não possuem energia suficiente para remover os elétrons dos átomos com os quais interagem (Heinrich, 2002), tais como as que variam dentro do espectro do ultravioleta, da luz visível, do infravermelho, das micro-ondas e às das radiações eletromagnéticas utilizadas em sistemas de telecomunicações.

TABELA 1 Características das várias regiões do espectro eletromagnético.

	Comprimento de onda (m)	Frequência (Hz)	Energia (J)
Rádio	$> 1x10^{-1}$	$< 3x10^{9}$	$< 2x10^{-24}$
Micro-ondas	$1x10^{-3}$ a $1x10^{-1}$	$3x10^{9}$ a $3x10^{11}$	$2x10^{-24}$ a $2x10^{-22}$
Infravermelho	$7x10^{-7}$ a $1x10^{-3}$	$3x10^{11}$ a 410^{14}	$2x10^{-22}$ a $3x10^{-19}$
Visível	$4x10^{-7}$ a $7x10^{-7}$	$4x10^{14}$ a $7,5x10^{14}$	$3x10^{-19}$ a $5x10^{-19}$
UV	$1x10^{-8}$ a $4x10^{-7}$	$7,5x10^{14}$ a $3x10^{16}$	$5x10^{-19}$ a $2x10^{-17}$
Raio X	$1x10^{-11}$ a $1x10^{-8}$	$3x10^{16}$ a $3x10^{19}$	$2x10^{-17}$ a $2x10^{-14}$

	Comprimento de onda (m)	Frequência (Hz)	Energia (J)
Gama	$< 1x10^{-11}$	$> 3x10^{19}$	$> 2x10^{-14}$

Fonte: (Nasa, 2017).

Segundo Catalão (2010), o espectro das radiações não ionizantes abarca três áreas:

a) a primeira se refere aos campos eletromagnéticos de frequências extremamente baixas, que não ultrapassam a casa dos 3 x 103 Hz;

b) a segunda, diz respeito à radiação de radiofrequência, foco deste trabalho, a qual constitui ondas eletromagnéticas que se propagam no ar e no vácuo entre 3 x 103 Hz e 3 x 1011 Hz, ou seja, compreendendo as ondas de rádio e as micro-ondas;

c) finalmente a terceira reporta-se à radiação infravermelha (IV), a radiação visível, capaz de sensibilizar os olhos humanos e também à radiação ultravioleta (UV).

2.1.2 Radiofrequências

Segundo Catalão (2010) o termo radiofrequência (RF) refere-se a uma corrente alternada que, se for fornecida por uma antena, gera campos eletromagnéticos, adequados para serem utilizados em comunicações. A subdivisão dessa parte do espectro eletromagnético acontece conforme o Quadro 1:

QUADRO 1 O espectro das radiofrequências.

Legenda	Descrição	Frequência (Hz)
VLF	Frequência muito baixa	$3x10^3$ a $3x10^4$
LF	Frequência baixa	$3x10^4$ a $3x10^5$
MF	Frequência média	$3x10^5$ a $3x10^6$
HF	Frequência alta	$3x10^6$ a $3x10^7$
VHF	Frequência muito alta	$3x10^7$ a $3x10^8$
UHF	Frequência ultra alta	$3x10^8$ a $3x10^9$
SHF	Frequência super alta	$3x10^9$ a $3x10^{10}$
EHF	Frequência extremamente alta	$3x10^{10}$ a $3x10^{11}$

Fonte: (BRASIL, 2002).

2.2 EFEITOS BIOLÓGICOS DAS RADIAÇÕES NÃO IONIZANTES

Se um indivíduo for atingido por um feixe de radiação não ionizante, não ocorrerá nenhuma lesão visível no momento da irradiação, por isso não se percebe quando se é irradiado.

Contudo, antes de se definir os efeitos que cada radiação provoca nos seres humanos, necessário é explicar o trinômio ao qual se pode ter a chance de se desenvolver algum resultado expressivo.

Primeiramente, deve-se ter em mente que não é porque as pessoas se submetem a Campos Elétricos e Magnéticos (CEM) que vão desenvolver algum efeito físico ou biológico. Fatores combinados como a energia da radiação, o tempo de exposição, a dose absorvida, a parte do corpo atingida e a própria sensibilidade da pessoa devem ser estudados para se supor ou analisar um possível efeito.

Para analisar o resultado obtido, são necessários os seguintes parâmetros:

a) intensidade do CEM - A quantidade de energia que um material poderá absorver a partir da radiação a que se encontra sujeito depende da frequência da radiação e da intensidade do feixe (CATALÃO, 2010);

b) tempo de exposição ao CEM - O tempo de exposição em pessoas aumenta proporcionalmente a probabilidade de manifestação de algum efeito indesejado ao longo do tempo, pois com isso se aumenta a dose absorvida. Tanto que a Comissão Internacional de Proteção Contra Radiação Não Ionizante (ICNIRP) limita o tempo de permanência à exposição ocupacional, baseado no Comunicado de Imprensa nº 208 da OMS/IARC (Organização Mundial

da Saúde / Agência Internacional de Pesquisa em Câncer) que classificou os CEM providos de radiofrequências em possivelmente carcinogênicos a humanos (OMS, 2011);

c) susceptibilidade do organismo em se desenvolver algum efeito nocivo ou não. A susceptibilidade em ser afetado é a tendência do corpo a desenvolver algo nocivo ou sofrer um efeito qualquer. Cada pessoa reage de forma distinta ante uma exposição, cada parte do corpo possui diferentes sensibilidades, cada um possui diferenças naturais físicas e bioquímicas. Enfim, existem pessoas mais sensíveis que outras, fato que torna imprevisível e mutável os efeitos, o que impossibilita generalizações. (BELLAVITE, 2002).

3.2.1 Bioeletromagnetismo

A medida de referência para a absorção de energia eletromagnética, até 10 GHz, é a chamada taxa de absorção específica (SAR) (MOUTINHO & TELES, 2005), que mede o ritmo com que a energia é absorvida por unidade de massa de tecido biológico, e se expressa em Watts por quilograma.

Segundo Paulino (2001), a taxa de absorção de energia depende da densidade de potência da radiação eletromagnética e das características do tecido onde a radiação incide. Assim, a SAR quantifica a energia absorvida pelo tecido, sendo diretamente proporcional ao aumento local de temperatura, ou seja, quanto maior a SAR, maior o aumento da temperatura.

Moutinho e Teles (2005) exibem que diversos estudos epidemiológicos têm sido realizados a fim de evidenciar os efeitos das radiações não ionizantes em seres humanos. Como exemplo, mostra-se que humanos em descanso a uma SAR sobre todo o corpo entre 1 a 4 Watts por quilograma, durante um intervalo de 30 minutos, tiveram um aumento da temperatura corporal inferior a 1 ºC, o que propiciou desconforto nas pessoas em estudo.

Excedendo valores a 4 Watts por quilograma, o organismo perde a capacidade natural de termorregulação, o que leva a um aumento de temperatura corporal superior a 2 ºC suficiente para causar efeitos clínicos.

3.2.2 Possíveis efeitos

Ribeiro & Pessoa (2007) demonstram que estudos recentes chegaram à conclusão de que há a possibilidade do surgimento de patologias associadas ao aumento da temperatura corporal gerada por efeito termohidráulico a seguir:

Os olhos são considerados uma área crítica, com relação ao efeito das radiações não ionizantes, sendo bastante suscetível ao efeito térmico. Quantidades relativamente pequenas de energia eletromagnética podem elevar a temperatura das lentes oculares, pelo fato destas não possuírem sistema vascular adequado para as trocas térmicas, o que reduz sua capacidade de dissipação de calor. Por isso, a possibilidade de danos aos olhos constitui um aspecto muito sério das radiações de micro-ondas e radiofrequência (LAMPARELLI, 1998).

Os testículos também constituem órgãos críticos no que concerne aos efeitos das radiações eletromagnéticas. Isso porque são extremamente sensíveis a elevações de temperatura. Estão mais sujeitos à radiação por dois motivos: localização superficial em relação ao corpo e grande sensibilidade ao calor por parte das células germinativas, que se encontram em torno dos 33 graus Celsius. Assim, ao expor os militares da Arma de Comunicações às micro-ondas, os combatentes se sujeitam a um possível enfraquecimento da função reprodutiva, pois os testículos estarão fora do ambiente ideal para que se mantenha a homeostase do ciclo de produção de células reprodutivas (LAMPARELLI, 1998).

O sistema auditivo também pode ser afetado pelas RFs através do chamado efeito

de audição de micro-ondas ou “Efeito Frey” em homenagem ao neurocientista Allan H. Frey que estudou esse fenômeno profundamente e foi o primeiro a publicar informações sobre a natureza do efeito auditivo de micro-ondas. O Efeito Frey consiste de estalidos audíveis ou zumbidos induzidos por pulsos de frequências de micro-ondas. Esse efeito ocorre como resultado da expansão térmica de partes do ouvido humano em torno da cóclea, mesmo mediante muito baixa densidade de potência. Esta resposta do sistema auditivo ocorre para a faixa de frequência desde 2 x 108 Hz até pelo menos 3 x 109 Hz (JUSTESEN, 1975).

Além dos sintomas supracitados, diversos trabalhos indexados e de bom nível conseguiram demonstrar o aumento da ocorrência de vários tipos de sintomas em trabalhadores expostos a campos eletromagnéticos tais como: mal estar geral, dores de cabeça, nervosismo exagerado, insônia, depressão, angustia, diminuição da memória e da concentração, fraqueza e indisposição (FELIPPE JR, 2000).

3.3 LEGISLAÇÃO

Em 1996, a OMS implantou o projeto internacional de campos eletromagnéticos para investigar os potenciais riscos para a saúde associados a tecnologias emissoras de campos elétricos e magnéticos, baseado nisso, no mesmo ano a Associação Brasileira de Compatibilidade Eletromagnética (ABRICEM) tentou regulamentar a exposição humana a campos elétricos, magnéticos e eletromagnéticos de radiofrequências entre 9 x 103 Hz e 3 x 108 GHz. Isso teve como resultado uma proposta de normatização que foi adotada pela Agência Nacional de Telecomunicações (ANATEL) através da publicação da resolução n° 303, de 2 de julho de 2002, que estipula limites para exposição humana a campos elétricos, magnéticos e eletromagnéticos de radiofrequência (BELARDO, 2004).

As discussões sobre o tema se amadureceram até que o Brasil aprovou a Lei n. º 11.934, de 5 de maio de 2009, que se baseou em estudos da OMS sobre a taxação de limites referentes à exposição a campos eletromagnéticos e na prevenção dos efeitos adversos por eles causados, como o efeito térmico, por exemplo.

No caput do Art. 1º da referida lei depreende-se que ela estabelece limites à exposição humana a campos elétricos, magnéticos e eletromagnéticos, associados ao funcionamento de estações transmissoras de radiocomunicação, de terminais de usuário e de sistemas de energia elétrica nas faixas de frequências até 3 x 108 Hz, visando garantir a proteção da saúde e do meio ambiente (BRASIL, 2009).

O anexo da resolução nº 533, de 10 de setembro de 2009 da ANATEL, na parte número dois, inciso terceiro, relatava o

> Regulamento sobre limitação da exposição a campos elétricos, magnéticos e eletromagnéticos na faixa de radiofrequências entre 9 x 103 Hz e 3 x 108 Hz,

contudo, tal regulamento foi revogado pela Resolução nº 686, de 13 de outubro de 2017, tendo em vista o rápido avanço tecnológico dos meios de comunicação. Assim, a certificação e homologação de equipamentos a partir dessa data se dão por meio de portarias da ANATEL, permanecendo em vigor os limites de exposição constantes da resolução nº 303.

O anexo VII – Radiações Não Ionizantes, da Norma Regulamentadora número 15 (NR 15 – Atividades e Operações Insalubres) do Ministério do Trabalho estabelece que:

> As operações ou atividades que exponham os trabalhadores às radiações não ionizantes, sem a proteção adequada, serão consideradas insalubres, em decorrência de laudo de inspeção realizada no local de trabalho.(NR, 2009).

Assim, se as medições de campo indicarem valores de exposição superiores aos estabelecidos na resolução nº 303 da ANATEL, será devido ao adicional de insalubridade.

Por outro lado, a Portaria nº 206 – De-

partamento Geral do Pessoal (DGP), de 17 de dezembro de 2003, no artigo 1º, aprova as normas para concessão do adicional de compensação orgânica aos militares que desempenham atividades sujeitas apenas à radiação ionizante.

Essa proposta teve por objetivo proteger os militares e compensá-los financeiramente, pois foi estipulado um tempo limite diário e semanal à exposição às radiações. Além disso, foi incorporado ao soldo um percentual de 10% aos que manipulam substâncias radioativas ou que usam Raios-X, como exemplo, os Instrutores da EsIE e os profissionais da área de saúde.

Nessa linha, é válida a preocupação em atribuir 10% ao soldo militar como compensação orgânica, porém, este percentual não é aplicado aos que se expõem ao espectro não ionizante.

CONCLUSÃO

É possível constatar que os estudos nessa área da Ciência são recentes e seus resultados geram interesses tanto em fabricantes de equipamentos que emitem radiofrequências e micro-ondas, quanto naqueles que os operam, em especial, os militares.

É imperioso destacar que o conhecimento prévio do espectro eletromagnético motiva a percepção do indivíduo a sentir os possíveis efeitos e isso evita uma eventual negligência de superiores hierárquicos ao exporem seus subordinados de maneira excessiva nas missões a que cada brigada concorre.

Em seu Trabalho de Conclusão de Curso, o Autor (2017) conclui que os militares das escolas de formação, em especial os da AMAN, necessitam ser mais bem instruídos sobre o tema relativo às radiações não ionizantes e seus possíveis efeitos biológicos, para que seja possível planejar operações com emprego de militares escalados de forma melhor planejada, priorizando a salubridade dos subordinados.

Diante disso, medidas simples, como a confecção de uma escala de missão, com objetivo de controlar a frequência de emprego de cada militar em cada operação, tornam-se eficientes ferramentas para a minimização da exposição e, consequentemente, da possibilidade de se desenvolver alguns dos possíveis efeitos estudados.

Vale notar que mesmo estando isento da necessidade de avaliação e de licenciamento para funcionamento, as estações transmissoras de radiocomunicação do EB não estão livres do atendimento aos limites de exposição estabelecidos por lei (ANATEL, 2002). Dessa maneira, é juridicamente importante que se faça o atendimento a tais normativas de maneira a mitigar possíveis impactos para a Força seja em razão do aumento na frequência de atendimentos médicos, da indisponibilidade, mesmo que temporária, de militar especializado, ou até mesmo com o pagamento de indenizações. Todas essas medidas têm, como objetivo último, propiciar um meio ambiente de trabalho salutar, direito de todo trabalhador.

POSSIBLE EFFECTS OF NON-IONIZING RADIATION ON MILITARY PERSONNEL IN THE BRAZILIAN ARMY

ABSTRACT. THIS PAPER IS A BRIEF STUDY ON THE EFFECTS OF NON-IONIZING RADIATION ON MILITARY PERSONNEL OF THE BRAZILIAN ARMY, AS WELL AS ON THE LEGAL ASPECTS OF THE ISSUE. THE RESEARCH RELIES ON THE LEVERAGE OF DATA OBTAINED THROUGH THEORETICAL ANALYSIS THAT SERVED AS A BASIS FOR THE IDENTIFICATION OF THE CHARACTERISTICS OF ELECTROMAGNETIC SPECTRUM AND VERIFICATION OF ITS POSSIBLE EFFECTS, AIMING AT THE IMPROVEMENT IN THE INSTRUCTIONS OF AMAN SIGNAL CORPS CADETS AND OF TROOPS THAT OPERATE THE MOST DIVERSE MEANS OF COMMUNICATIONS OF THE BRAZILIAN ARMY

KEYWORDS. NON-IONIZING RADIATION. BIOLOGICAL EFFECTS. STOCHASTIC EFFECTS.

REFERÊNCIAS

ANATEL, Agência Nacional de Telecomunicações. Regulamento sobre Limitação da Exposição a Campos Elétricos, Magnéticos e Eletromagnéticos na Faixa de Radiofrequências entre 9 kHz e 300 GHz. Resolução nº 303, de 2 de julho de 2002. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/17-2002/128-

resolucao-303> Acesso em: 22 mai. 18.

BELARDO, C. A. et. al. Exposição Humana a Campos Elétricos e Magnéticos Gerados por Instalações Elétricas 50 e 60 Hz., 2004. Disponível em: < http://www.mfap.com.br/pesquisa/arquivos/20081117111935-41.pdf>. Acesso em: 17 fev. 2017.

BELLAVITE, Paolo. Medicina Biodinâmica, a força vital suas patologias e suas terapias. 1. ed. Campinas, SP: Papirus, 2002.

BRASIL. Ministério da Defesa. Exército Brasileiro. C 24-2: administração de radiofrequências. 2. ed. Brasília: EGGCF, 2002.

BRASIL. Lei n. º 11.934, de 5 de maio de 2009. Dispõe sobre limites à exposição humana a campos elétricos, magnéticos e eletromagnéticos; altera a Lei n. º 4.771, de 15 de setembro de 1965; e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 5 de maio de 2009. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l11934.htm>. Acesso em: 20 set. 2016.

CATALÃO, João Paulo da Silva. Campos Eletromagnéticos em Sistemas Biológicos: Apontamento das Aulas Teóricas. Universidade da Beira Interior, Portugal, set. 2010. Disponível em: <http://webx.ubi.pt/~catalao/Apont_Campos.pdf>. Acesso em: 15 fev. 2017.

FELIPPE JUNIOR, J. Bio-Eletromagnetismo: Medicina Com Base Na Biofísica. 2000.Disponível em: <http://www.medicinabiomolecular.com.br/sdi4/sdi4-arquivos/pdf/tema57.pdf> . Acesso em: 14 mai 2018.

HEINRICH, Ralph Robert. Conceitos Básicos Sobre Radiações Não-ionizantes e seus Efeitos Potenciais sobre a Saúde Humana. 9 jul. 2002. Disponível em: <http://www.cram.org.br/wordpress/?p=1254>. Acesso em: 10 set. 2016.

JUSTESEN, D. R Microwaves and Behavior, The American Psychologist, vol 30, nr 3, 1975.

LAMPARELLI, Claudia Conde. et al. Radiações de micro-ondas e radiofrequência. Revista ambiente, vol. 2, n. 1, 1998.

MOUTINHO, P. F. A.; TELES, D. J.A. Exposição a campos eletromagnéticos: visão geral sobre o “estado da arte”. Portugal: FEUP, mar. 2005. Disponível em: <http://paginas.fe.up.pt/~ee00052/Relatorio_projecto_fase1.pdf>. Acesso em: 24 fev. 2017.

NASA, National Aeronautics and Space Administration, Goddard Space Flight Center. Imagine the Universe. Disponível em: https://imagine.gsfc.nasa.gov/science/toolbox/spectrum_chart.html Acesso: 14-JUL-2017

NR, Norma Regulamentadora Ministério do Trabalho e Emprego. NR-15 - Atividades e Operações Insalubres. 2009.

OMS – Organização Mundial da Saúde. Ficha Informativa n. º 232: jun. 2007. Disponível em:<http://www.OMS.int/peh-emf/publications/facts/fs322_ELF_fields_portuguese.pdf>. Acesso em: 11 fev. 2017.

PAULINO, J. O. S. Radiações Eletromagnéticas Não Ionizantes emitidas pelas Antenas Fixas de Telefonia Celular. Departamento de Engenharia Elétrica – Escola de Engenharia, Universidade Federal de Minas Gerais, 2001

RIBEIRO, Edson Leite; PESSOA, Martha Bulcão. Efeitos da radiação eletromagnética na vida do ser humano: uma análise do paradigma ambiental. Revista Tecnologia e Sociedade, v. 3, n. 5 (2007). Disponível em: <https://periodicos.utfpr.edu.br/rts/article/download/2502/1616>. Acesso em: 20 fev. 2017.

SILVA, Gabriel Pascoal Zanateli Zappi. Estudo dos possíveis efeitos das radiações não-ionizantes em militares do Exército Brasileiro. Trabalho de Conclusão de Curso – Ciências Militares, Academia Militar das Agulhas Negras – AMAN, 2017. Disponível em: <http://bdex.eb.mil.br/jspui/handle/1/1147> Acesso em: 22 mai. 18.

Gabriel Pascoal Zanateli Zappi Silva é Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (2017), possui os estágios de Cibernética pelo CIGE e Operações de Garantia da Lei e da Ordem pelo CIOpGLO. Serve atualmente no 1º BGE, em Brasília/DF e pode ser contactado pelo email gabriel.pzzs@hotmail.com.

Anderson Gomes de Jesus é Licenciado em Química pela Universidade Federal do Rio de Janeiro (2004) e Bacharel em Química pela Universidade do Grande Rio (2006), fez Mestrado em Ciência e Tecnologia Nucleares pelo Instituto de Engenharia Nuclear - IEN/CNEN (2017). Atua como Coordenador Adjunto de Aperfeiçoamento Docente, Professor e Orientador na Academia Militar das Agulhas Negras e pode ser contactado pelo email jesus.anderson@aman.eb.mil.br.

CICAD.I.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

INFORMÁTICA

ANÁLISE DE SEGURANÇA SOBRE APLICATIVO DE MENSAGEM INSTANTÂNEA: WHATSAPP COMO ESTUDO DE CASO

Antonio Marcos de Castro Mota[1], Paulo Roberto Corrêa Leão[2]
Pós-graduado em Perícia Computacional[1], Mestre em Gestão do Conhecimento e Tecnologia da Informação[2]

RESUMO: O vazamento de informações da agência norte-americana NSA (National Security Agency) por um de seus analistas, Edward Snowden, em 2013, trouxe à tona múltiplas informações sobre programas de vigilância e monitoramento de comunicações digitais geridos pela agência e que tinham como parceiros grandes provedores da Internet. Tal episódio, desencadeador de grande repercussão na comunidade internacional, instigou ainda mais precauções e cuidados por parte dos gestores e especialistas em segurança de comunicações, sobretudo quanto à necessidade de robustecimento de práticas relativas à salvaguarda de privacidade de dados na grande rede. Em meio a esse contexto, dada a popularização de ferramentas de troca de mensagens e do aumento do tráfego de voz sob IP em dispositivos móveis, uma pesquisa a respeito dos aspectos de segurança envolvidos nesse tipo de serviço, bem como um estudo de caso realizado sobre o WhatsApp (com enfoque no tráfego de dados e na quebra de privacidade e autenticidade) poderia resultar em importante conhecimento a ser compartilhado e divulgado à imensa quantidade de usuários finais da ferramenta, bem como aos estudiosos da área de Segurança e de Perícia Forense. Assim, o Artigo Técnico proposto referenciou o funcionamento das comunicações de voz sobre IP, percorrendo os principais métodos de criptografia e os atributos de segurança da informação. Para a realização do estudo empírico foi realizada uma pesquisa exploratória, tendo por base a pesquisa aplicada, a revisão bibliográfica, os padrões conhecidos sobre o tema e um estudo de caso seguido da respectiva análise e conclusão.

Palavras-chave: Segurança da Comunicação. VoIP. Forense Computacional. Análise de Tráfego.

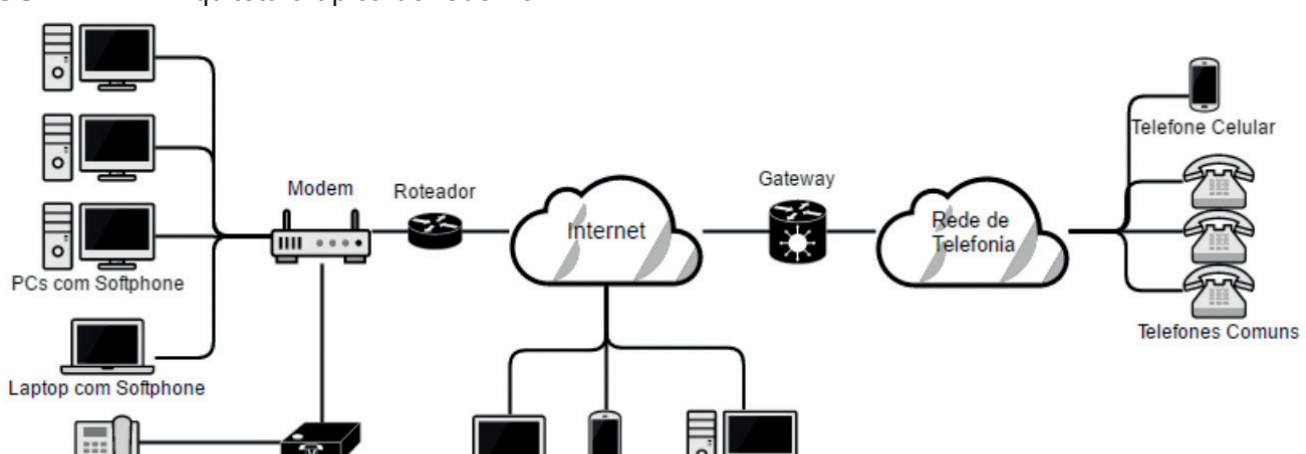
INTRODUÇÃO

Os aplicativos de mensagens instantâneas passaram por um amplo processo de massificação nesta última década. Em busca de tornar os softwares mensageiros atrativos, as empresas desenvolvedoras passaram a agregar várias funcionalidades aos seus projetos de comunicação, assim, além do envio de textos, tornou-se possível em um mesmo aplicativo a troca de arquivos como gifs animados, planilhas, documentos em formato portátil, músicas, entre outras.

A integração de chamadas de voz sobre IP (VoIP) aos softwares de troca de mensagens, certamente foi um dos mais importantes passos na ampliação dessa convergência de serviços em aparelhos telefônicos.

Os sistemas VoIP trazem inúmeras vantagens, tais como redução de custo operacional (em virtude de uma mesma rede para transporte de dados e voz), flexibilidade (uma vez que proporciona grande variedade de serviços), mobilidade (pois usuários podem fazer e receber chamadas de voz a partir de uma infinidade de pontos geográficos), entre outras características. Na Figura 1 estão elencadas algumas possibilidades de interconexão de dispositivos VoIP.

FIGURA 1 Arquitetura típica de rede VoIP.



Fonte: o autor, 2016.

À medida que tais aplicativos de mensagens (e voz) tornaram-se amplamente utilizados cresceram também os problemas relacionados à segurança. A interceptação de sinais, a invasão de dispositivo e a popularização de métodos de crimes cibernéticos são fatores que demonstram a necessidade do aprofundamento de estudos que envolvam o envio e recebimento de tráfego de dados e VoIP, bem como de medidas que possam mitigar possíveis ataques ou ameaças.

> Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e as oportunidades de negócio. (NBR ISO 27002/2005, p. 10).

Assim, pesquisas atinentes à segurança das informações em tais tipos de softwares revestem-se de relevância, vez que podem vir a subsidiar novas técnicas, metodologias, códigos e “retratos” que visem aprimorar os cuidados com as comunicações de dados e de voz sobre IP.

Este artigo tem como objetivo geral a elaboração de uma análise de segurança de informações sobre um aplicativo de mensagem instantânea. Para tanto, montou-se uma rede privada (em laboratório) em que foram colocados em prática métodos de análise de tráfego e MAC spoofing objetivando-se levantar e identificar possíveis brechas.

A organização deste escrito estrutura-se da seguinte forma: a seção 2 trata da metodologia da pesquisa, dos instrumentos e procedimentos, bem como da pormenorização do estudo de caso em si; a seção 3 trata dos resultados e discussões; e a seção 4 exibe a parte final com as conclusões do autor sobre o tema estudado.

1 METODOLOGIA E MATERIAIS

A seguir estão elencados o tipo de metodologia aplicada, os instrumentos, os procedimentos e a implementação do estudo de caso.

1.1 METODOLOGIA

Para subsidiar este artigo realizou-se uma pesquisa bibliográfica em meio a literatura de tecnologia da informação sobre assuntos como segurança da informação, criptografia e VoIP.

Foram realizadas também consultas em artigos e trabalhos de conclusão de curso, bem como explorações em sites especializados da internet.

> Determinados o objetivo da pesquisa e a abordagem científica que irá orientar a investigação, é necessário decidir que método de pesquisa melhor se aplica à condução do estudo. (DRESCH, 2015, p. 16).

Conforme a mesma autora, pode-se

dizer que o artigo em questão está enquadrado conforme os seguintes tipos científicos elencados:

a) quanto à natureza – trata-se de uma pesquisa aplicada a Sistemas de Informação;

b) quanto à forma de abordagem do problema – trata-se de uma pesquisa qualitativa, realizada com o objetivo de levantar o envio e recebimento de dados de voz e texto e a constatação da camada de segurança;

c) quanto aos fins – trata-se de uma pesquisa descritiva, pois busca expor algumas características de segurança em aplicativo de uso generalizado; e

d) quanto aos meios – trata-se de um estudo de caso, pois aprofunda-se na análise da segurança das informações trafegáveis em um ambiente montado e dedicado para tal finalidade.

1.2 INSTRUMENTOS E PROCEDIMENTOS

Para a execução do estudo de caso foi montado um ambiente de testes em que se utilizaram os dispositivos a seguir:

- dois celulares Motorola Moto G 2014 XT 1064 8GB (2ª Geração) (SO Android 5.0.2);
- um notebook Lenovo G40-70 (SO Windows 10); e
- um notebook Dell Inspiron 14 (SO Windows 8.1).

Ambos celulares utilizados nesse estudo possuíam o aplicativo WhatsApp (versão 2.12.539 para Motorola) instalado em seus sistemas. Os notebooks tinham acesso ao WhatsApp Web que é uma variante do mensageiro e que podem ser acessadas por browsers (desde que ocorra uma autenticação por meio de um QR Code). As mensagens enviadas e recebidas são completamente sincronizadas entre o aplicativo de um aparelho celular e o computador, podendo ser vistas em ambos dispositivos.

1.3 ESTUDO DE CASO

Este estudo de caso pretende demonstrar a possibilidade de se duplicar a conta de WhatsApp de um usuário que pertence a uma mesma rede de um falsário. Dessa forma, seria possível a um falsário ter acesso às mensagens e contatos da vítima a partir de outro celular.

De acordo com o método utilizado, se faz necessário a aquisição do endereço MAC (Media Access Control) do telefone do usuário alvo. O MAC é um endereço único, com 12 dígitos hexadecimais que identifica a placa de rede do dispositivo.

Neste teste, os dispositivos (celulares e notebooks) estão ligados a uma mesma rede local e conectados a um modem, o que torna possível o uso de um programa como o Wireshark, que é um analisador de protocolos e que permite a captura e navegação interativa no tráfego de uma rede de computadores em tempo de execução, para esmiuçar a rede e descobrir o endereço MAC do smartphone do usuário alvo.

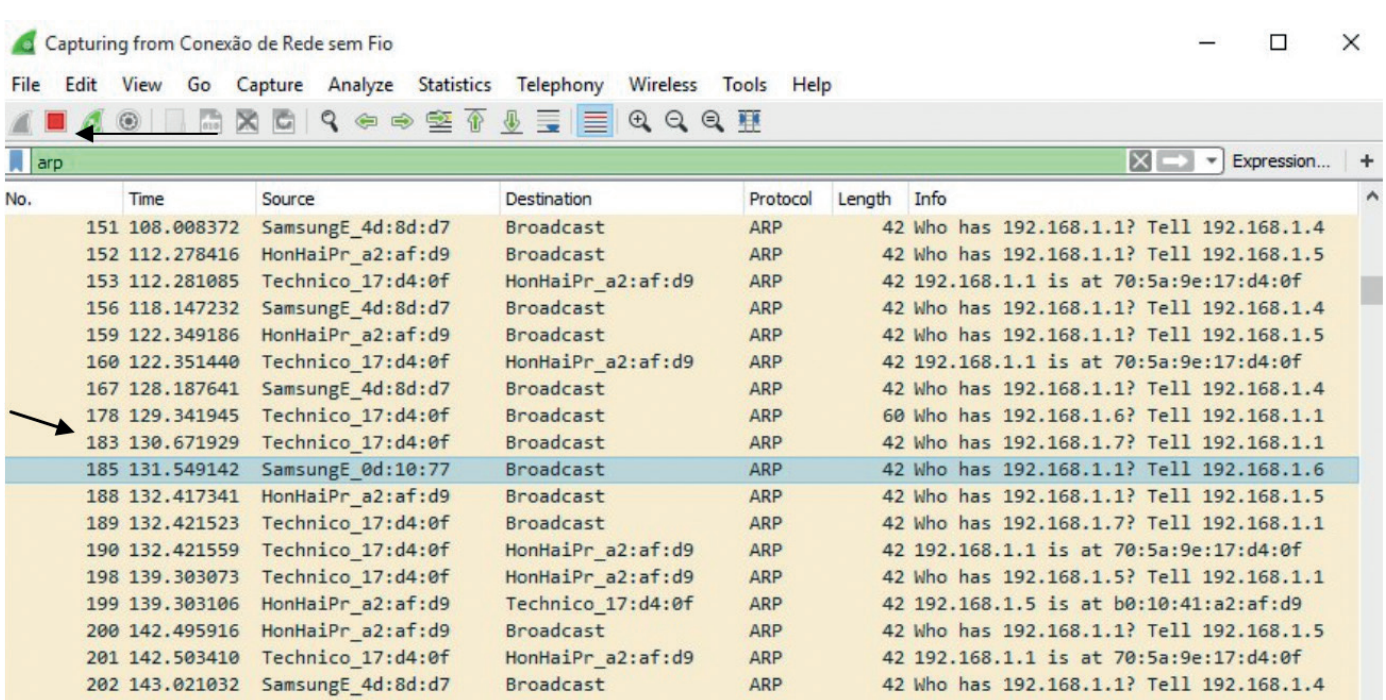
O protocolo ARP (Address Resolution Protocol) permite conhecer o endereço físico de uma placa de rede que corresponde a um endereço IP.

Para fazer a correspondência entre os endereços físicos registrados nas placas de rede pelos fabricantes (MAC) e os endereços lógicos (IP), o protocolo ARP interroga as demais máquinas da rede em busca do endereço físico.

Assim, com a utilização de um filtro, no programa Wireshark, que separe os pacotes por tipo de protocolo (e nesse caso queremos apenas ARP) é possível verificar o tráfego de todos os pacotes desejados. A Figura 2 mostra

o momento em que é realizada a captura.

FIGURA 2 Captura de pacotes de rede com protocolos do tipo ARP.

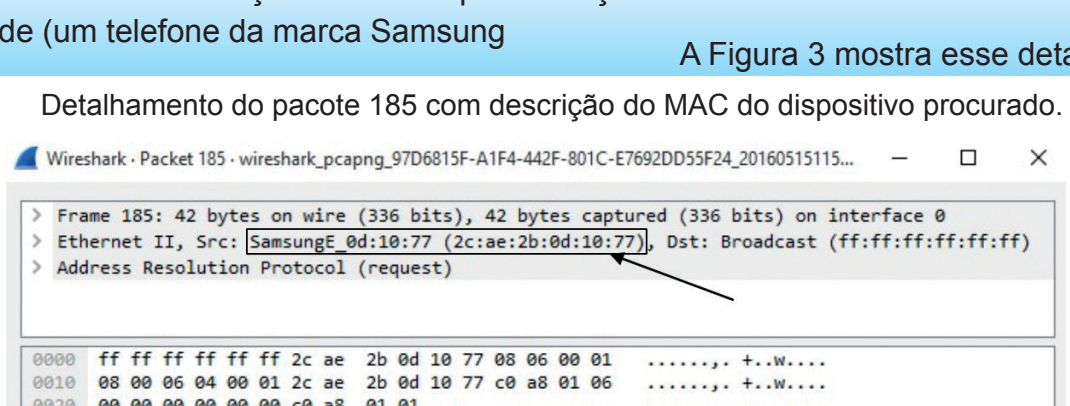


Fonte: o autor, 2016.

A partir da observação dos pacotes identifica-se o dispositivo que se deseja adquirir mais informações, no teste em questão estamos buscando o endereço MAC do dispositivo de rede (um telefone da marca Samsung e cujo número IP é o 192.168.1.6). Ao se identificar o pacote procurado podemos expandir suas informações para adquirirmos seu endereço MAC.

A Figura 3 mostra esse detalhamento.

FIGURA 3 Detalhamento do pacote 185 com descrição do MAC do dispositivo procurado.



Fonte: o autor, 2016.

De posse do endereço MAC da vítima e com acesso root no dispositivo que será utilizado para clonar a conta WhatsApp, se faz a atualização do endereço MAC do aparelho do falsário. Esse passo pode ser executado com o auxílio de um aplicativo que substitua ou mascare o endereço MAC original pelo endereço MAC da vítima.

Neste estudo de caso foi utilizado o software KingRoot para se obter privilégios de superusuário que permitissem a realização do mascaramento do endereço MAC.

Para finalizar a clonagem, reinstala-se o aplicativo WhatsApp no dispositivo do falsário.

Para que a instalação seja concluída é preciso ter em mãos o código de confirmação enviado por mensagem SMS. Importa ressaltar que o código é enviado para o aparelho que possui o chip correspondente ao número de telefone vinculado à conta do WhatsApp que se deseja clonar, neste caso ao celular da vítima.

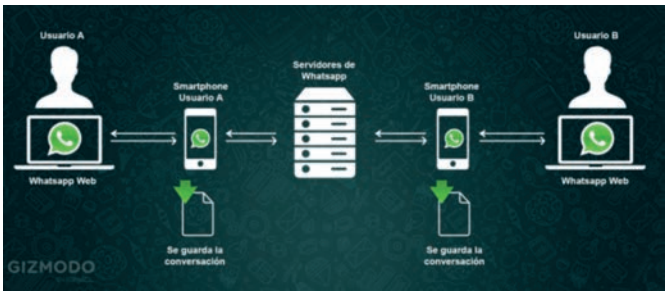
2 RESULTADOS E DISCUSSÕES

Com base em Anglano C. (2014), os serviços de mensagens instantâneas são cada vez mais usados, não só para atividades legítimas, mas também para ilícitas.

O WhatsApp é um aplicativo multiplataforma e possibilita a troca de mensagens entre diferentes dispositivos (celulares, tablets, notebooks etc.) e entre os mais variados sistemas operacionais, tais como Android, Windows, BlackBerry, iOS e outros.

A figura 4 exibe sua arquitetura de funcionamento.

FIGURA 4 Arquitetura de funcionamento do WhatsApp



Fonte: Gizmodo, 2015.

O WhatsApp, por ser líder de mercado, evidentemente torna-se alvo de cibercriminosos, logo, estudos voltados para a área de segurança da informação conjugados ao aplicativo citado fazem-se necessários.

De acordo com Goodrich et al (2013), tradicionalmente, a segurança da informação está relacionada com os seguintes atributos: confidencialidade, integridade, disponibilidade e autenticidade. É com base nestes atributos que estruturou-se a discussão construída nesta seção a partir dos resultados do estudo de caso.

Na seção 2 deste artigo, evidenciou-se a possibilidade da revelação não autorizada de dados contidos em conversas da conta clonada. Tal situação, indubitavelmente prejudica a confidencialidade na comunicação da vítima com seus contatos.

Al-Saadawi & Varol (2017) explicam que em redes IP, os dados são digitalizados e transmitidos em formato de pacotes. Tais pacotes são roteados baseados em alguns protocolos. No laboratório, a aquisição do endereço MAC do dispositivo alvo pôde ser efetuada porque o atacante estava conectado à mesma rede da vítima. Assim, o atacante de posse de um software analisador de rede pôde verificar todo o trâfego de pacotes.

> Um usuário com acesso a um terminal local pode tentar a intrusão sem usar uma rede intermediária. (...) Assim, a violação de sistemas é uma área na qual as preocupações relativas à segurança de rede e à segurança de computadores se sobrepõem. (STALLINGS, 2008).

No estudo de caso realizado, o atacante era parte da lista de usuários habilitados. Assim, podia “escutar” a rede. Tal situação, mesmo induzida (por ocasião da montagem do cenário do laboratório) traz à tona a importância da implementação do controle de acesso em redes privadas.

> O controle de acesso é a capacidade de limitar e dominar o acesso aos sistemas e aplicações por meio de links de comunicação. Para conseguir isso, cada entidade que tenta obter acesso precisa primeiro ser identificada, ou autenticada, de modo que os direitos de acessos possam ser ajustados ao indíviduo. (STALLINGS, 2008).

No caso de redes públicas totalmente abertas, a intecerptação de dados por cibercriminosos é ainda mais facilitada, motivo pelo qual especialistas recomendam a não utilização destes tipos de conexões para a execução de procedimentos críticos que envolvam informações sensíveis. Em redes privadas, o controle de acesso poderá ser mais uma ação

para mitigar adesões de usuários mal-intencionados.

O estudo de caso revelou, na versão estudada do aplicativo mensageiro, uma carência de atenção quanto à autenticação e autorização.

Para se completar a instalação e para se confirmar a identidade, a administração do WhatsApp encaminhava um token (enviado por SMS) que após ser digitado em campo específico habilitava o usuário a utilizar o aplicativo. Esse conjunto de procedimentos demonstrou-se pouco adequado para impedir que atacantes consiguissem o token, até porque, conforme preceituam Krombholz et al (2013), cibercriminosos têm lançado mão de ataques cada vez mais sofisticados, inclusive com o uso de engenharia social.

A despeito disso, versões posteriores do WhatsApp passaram a implementar verificação em duas etapas, com envio do token para o e-mail e com o cadastro de uma senha como "recurso opcional" para situações em que os usuários necessitem instalar o programa novamente.

Importa ressaltar que o laboratório fora realizado em ambiente isolado e que a metodologia de duplicação de conta descrita neste artigo talvez não seja bem-sucedida ao ser aplicada em aparelhos pertencentes a redes diferentes.

Hoje, existem diversos métodos para se conseguir endereços MAC de maneira não-autorizada. Como preceitua Mota Filho (2013), a análise de tráfego em redes TCP/IP permite entre outras possibilidades: monitorar relevantes mensagens de sistema não reveladas pelas aplicações, bem como instruir-se sobre o funcionamento de protocolos e serviços pela observação. O software Wireshark utilizado no estudo de caso possibilitou realizar a análise dos dados que trafegavam na rede. Filtrando-se o protocolo ARP, o atacante conseguiu, sem muita dificuldade, importantes informações como o endereço IP e o endereço MAC do dispositivo alvo.

Também é perfeitamente possível duplicar os endereços físicos das placas de rede. A utilização de aplicativos é uma das formas de se chegar a esse objetivo conforme ficou demonstrado no estudo. Existem inclusive dispositivos piratas que vêm de fábrica com a numeração de suas placas de rede já duplicadas.

Por ocasião da execução do estudo de caso, o dispositivo (do falsário) utilizado para se alterar o número MAC e para se clonar a conta do WhatsApp apresentou problemas em seu sistema operacional quando foi reinicializado, provavelmente em função de conflitos quanto ao reconhecimento do MAC modificado, o que exigiu a reconfiguração de fábrica para restabelecer as funcionalidades do aparelho celular.

Outro aspecto da segurança da informação comprometido foi a integridade dos dados. No profile clonado foi possível interferir em conversas de forma não autorizada.

Por fim, quanto à disponibilidade do serviço, este funcionou por todo o período dos testes. Não houveram tentativas de tirá-lo do ar.

CONCLUSÃO

Com mais de um bilhão de usuários ativos (informação essa divulgada em fevereiro de 2016 pela própria empresa), o WhatsApp bem como outros serviços de mensagem tende a contar por muito tempo ainda com índices elevados de popularidade e adesão aos seus serviços.

Toda essa notoriedade acaba por tornar o aplicativo de mensagens um grande atrativo para pessoas mal-intencionadas e organizações criminosas que enxergam no elevado número de usuários possibilidades infinitas para o cometimento de crimes.

Por mais que as empresas desenvolvedoras invistam pesado na criação e aperfeiçoamento de metodologias para mitigação de riscos, o aumento no nível de segurança não necessariamente garante a segurança total dos sistemas.

Não é por acaso que quase diariamente são veiculados noticiários e divulgações de novas vulnerabilidades, malwares, ameaças e brechas.

O WhatsApp é um aplicativo de mensagens multiplataforma, que tem um modelo negocial de baixo ou nenhum custo para seus usuários, apresenta relativa facilidade de uso e possui um enorme tráfego de dados entre os milhares de dispositivos que fazem uso de seus serviços. Por tudo isso tal tipo de programa apresenta-se como um relevante objeto de pesquisas.

O presente artigo foi realizado com a intenção de estudar e testar a aplicação e identificar possíveis falhas de segurança.

Para ajudar a subsidiar o escrito foi produzido um estudo teórico a respeito de voz sobre IP e segurança da computação.

O estudo de caso, descrito neste artigo, contemplou a análise de tráfego de dispositivos de uma mesma rede, onde foi possível capturar, com o auxílio de uma ferramenta de inspeção de pacotes, o número físico da placa de rede de um dos dispositivos.

Em seguida foi utilizado um software para rotear um aparelho de telefone e outro aplicativo para mascarar o endereço MAC. A partir daí foi possível instalar o WhatsApp de outro aparelho de telefone e ter acesso às informações de outro usuário.

Conclui-se que ainda é inteiramente possível fazer uso de técnicas para contornar a autenticidade dos usuários quando da instalação do aplicativo de mensageria WhatsApp. Além do mais, a partir do acesso à conta se pode consultar e enviar mensagens atacando também os princípios da privacidade e integridade de dados.

Por fim, destaca-se a importância de se aplicar sempre novas camadas de segurança em aparelhos e aplicativos com o objetivo contínuo de se incrementar possibilidades de segurança ao acesso de redes, aparelhos e softwares.

Sugere-se o estudo de metodologias de segurança e proteção aplicados a serviços e aplicativos de troca de mensagens.

Sugere-se também um Estudo de Caso que verifique a viabilidade de aquisição de endereço MAC e a duplicação de uma mesma conta do WhatsApp em dispositivos que pertençam a redes diferentes. Uma pesquisa sobre a eficiência de aplicativos e implementações que oferecem proteção e bloqueio a mensageiros e comunicadores instantâneos através de PIN e senhas também poderia ser de grande pertinência.

SECURITY ANALYSIS ON INSTANT MESSAGING APPLICATION: WHATSAPP AS CASE STUDY

Abstract. The leakage of information from the US National Security Agency (NSA) by one of its analysts, Edward Snowden, in 2013, brought to the forefront multiple information on surveillance and monitoring programs for digital communications managed by the agency and which had large partners providers. This event, which had a major impact on the international community, further instigated precautions by communications security managers and specialists, especially regarding the need to strengthen data protection practices in the large network. Given this context, due to the popularization of messaging tools and the increase of voice traffic under IP on mobile devices, a research on the security aspects involved in this type of service, as well as a case study carried out on WhatsApp (focusing on data traffic and breaking privacy and authenticity) could result in important knowledge to be shared and disseminated to the vast number of end-users of the tool, as well as scholars in the area of Security and Forensic Skills. Thus, the proposed technical article referred to the operation of voice over IP communications, covering the main methods of encryption and information security attributes. For the accomplishment of the empirical study an exploratory research was carried out, based on the applied research, the bibliographic revision, the known protocols on the subject and a case study followed by the respective analysis and conclusion.

Keyword: Communication Security. VoIP. Computational Forensics. Traffic Analysis. Instant Messaging Application.

REFERÊNCIAS

ABNT- Associação Brasileira de Normas Técnicas. NBR ISO 27.002/2005 – Tecnologia da Informação – **Técnicas de Segurança – Código de prática para a gestão de segurança da informação**. Rio de Janeiro, ABNT, 2004.

AL-SAADAWI, Hussein; VAROL, Asaf. **Voice over IP forensic approaches: A review**. Conference: 2017 5th International Symposium on Digital Forensic and Security. Romenia, 2017, DOI: 10.1109/ISDFS.2017.7916507

ANGLANO C, **Forensic analysis of WhatsApp Messenger on Android smartphones**, Digital Investigation, 2014, http://dx.doi.org/10.1016/j.diin.2014.04.003

BURNETT, Steve; PAINE, Stephen. **Criptografia e segurança**: o guia oficial RSA. Rio de Janeiro: Elsevier, 2002.

CARUSO, Carlos A. A; STEFFEN, Flávio D. **Segurança em informática e de informações**. 3ª ed. São Paulo: Editora Senac São Paulo, 2006.

DRESCH, Aline; LACERDA, Daniel P.; JUNIOR, José J.A.V.A. **Design Science Research – Método de pesquisa para avanço ciência e tecnologia**. Porto Alegre: Editora Bookman, 2015.

GOODRICH, Michael. T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. Porto Alegre: Bookman, 2013.

KROMBHOLZ, Katharina & Hobel, HEIDELINDE & Huber, MARKUS & Weippl, Edgar. **Social engineering attacks on the knowledge worker**. - Proceedings of the 6th International Conference on Security of Information and Networks, 2013. 10.1145/2523514.2523596

MOTA FILHO, João Eriberto. **Análise de tráfego em redes TCP/IP: utilize tcpdump na análise de tráfegos em qualquer sistema operacional**. São Paulo: Novatec Editora, 2013.

STALLINGS, William. **Criptografia e segurança de redes**. São Paulo: Pearson Prentice Hall, 2008.

Antonio Marcos de Castro Mota é graduado em Ciência da Computação (2008), pós-graduado em Perícia Digital (2016), ambas, junto à Universidade Católica de Brasília (UCB). Atualmente, trabalha na Divisão de Controle de Produtos Químicos, unidade integrante do Departamento de Polícia Federal, órgão em que ocupa cargo efetivo de Agente Administrativo e pode ser contactado pelo email antonio.amcm@dpf.gov.br.

Paulo Roberto Corrêa Leão é formado pela Academia Militar das Agulhas Negras (1977), pós-graduado em análise de sistemas, supervisão escolar, gestão estratégica da informação e mestrado em Gestão do Conhecimento e da Tecnologia da Informação, pela Universidade Católica de Brasília (2004). Atualmente está cursando o doutorado em Educação na Universidade Católica de Brasília(UCB).

CICAD.I.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

ENG. ELÉTRICA
TELECOMUNICAÇÕES

USO ESTRATÉGICO DE DADOS DE IONOSSONDAS PARA COMUNICAÇÕES DIGITAIS EM ALTA FREQUÊNCIA (HF)

Vítor Ossamu Rodrigues Okamura[1], Plínio Ricardo Ganime Alves[2]
Graduando em Engenharia Elétrica[1], Doutor em Engenharia Elétrica[2]

RESUMO: Este projeto apresenta um método computacional para otimizar transmissões de rádio de longa distância em alta frequência. Para comunicações de alta frequência, geralmente se faz uso de previsões ionosféricas mensais que, devido à anomalia ionosférica equatorial, não possuem exatidão satisfatória em regiões de baixa latitude, tornando impraticável seu uso em grandes porções do solo brasileiro. A iniciativa visa apresentar um procedimento alternativo para tornar estas comunicações eficientes nestas regiões do globo. Ao usar dados em tempo real de ionossondas, é possível aperfeiçoar estas transmissões calculando e ajustando instantaneamente seus parâmetros cruciais: a frequência máxima e o ângulo de take-off da antena. O trabalho busca oferecer um procedimento computacional eficiente, feito em C++ e baseado em interpolações e análise gráfica de ionogramas, para realizar os cálculos dessas grandezas com alta precisão e um algoritmo para lidar com as interrupções de longo prazo do funcionamento das ionossondas, selecionando dados anteriores congruentes com a hora e a época do ano atuais. Com o aprimoramento das transmissões em alta frequência por meio da proposta do projeto, busca-se viabilizar o uso do padrão Digital Radio Mondiale (DRM) de rádio, que possibilitaria comunicações multimídia acessíveis e seguras, de grande aplicação estratégica militar e civil, por todo o território nacional.

Palavras-chave: Digital Radio Mondiale. Transmissões de Rádio. Alta Frequência. Ionossonda. C++.

INTRODUÇÃO

Comunicações em alta frequência (HF) são costumeiramente baseadas em previsões ionosféricas mensais. Este método é pouco efetivo e utilizável em regiões de baixa latitude devido à anomalia de ionização equatorial (EIA), que faz com que mesmo previsões em curto prazo da camada ionosférica se tornem imprecisas, por causa da natureza caótica do fenômeno.

O objetivo do projeto é apresentar uma alternativa viável a estas previsões mensais usando dados em tempo real fornecidos por ionossondas para ajustar instantaneamente os parâmetros de transmissão, de forma a tornar comunicações de alta qualidade pelo padrão DRM em alta frequência realizáveis e eficientes para longas distâncias.

Possibilitar o uso eficaz desta tecnologia abre o caminho para diversas aplicações estratégicas. Ela é capaz de prover um canal seguro de comunicações para as partes mais remotas do território nacional, possibilitando uma forma econômica e confiável de coordenar e transmitir informações a operações militares na fronteira, entre outros usos.

O DRM é um padrão de rádio versátil, eficiente e de alta qualidade, livre de taxas de licenciamento devido à sua natureza livre, o que torna bastante desejável seu uso em várias aplicações civis, tais como prevenção de desastres, educação a distância e jornalismo multimídia, conforme avança a sua acessibilidade.

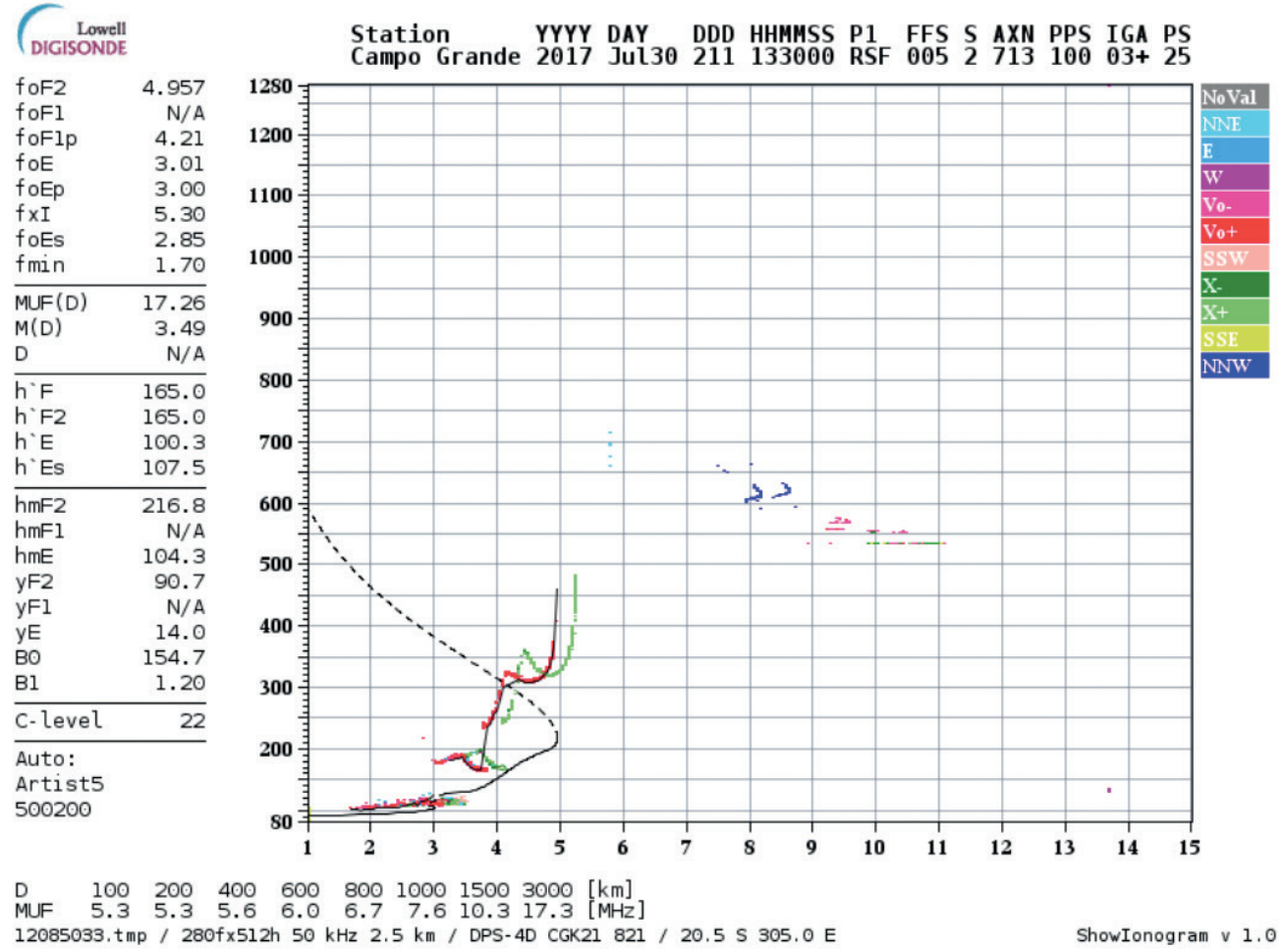
1 METODOLOGIA

1.1 CÁLCULO DE PARÂMETROS POR MEIO DE IONOGRAMAS

Queremos otimizar uma transmissão, entre dois pontos na superfície, separados por uma distância *D*, num dado horário, de rádio em alta frequência, rebatendo na camada io-

nosférica da atmosfera. Supomos que dispomos do ionograma (Figura 1) no ponto médio exato entre a origem do sinal (a antena transmissora) e o destino (a antena receptora).

FIGURA 1 Ionograma registrado pela ionossonda de Campo Grande no dia 30 de julho de 2017 às 13h30 UTC (09h30 no horário local).



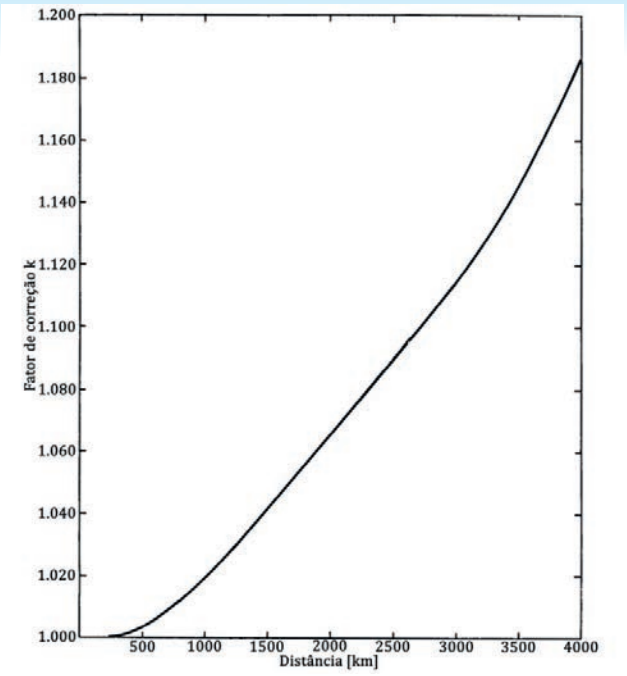
Fonte: GLOBAL IONOSPHERIC RADIO OBSERVATORY. Digital Ionogram DataBase. (2018)[2]

O ionograma nos fornece a altura virtual *h'* no ponto analisado em função da frequência f_v de uma onda vertical, aplicada perpendicularmente à ionosfera: esta é a curva *h'* x *f*, mostrada em vermelho no ionograma. Para uma propagação oblíqua, a frequência f_{ob} da transmissão é dada por

A constante *k* é um fator de correção, cujo valor depende da distância *D* e é obtido empiricamente (Figura 2).

$$f_{ob} = k f_v \sqrt{1 + \left(\frac{D}{2h'}\right)^2} \,. \qquad (1)$$

FIGURA 2 Fator de correção *k* em função da distância *D*.



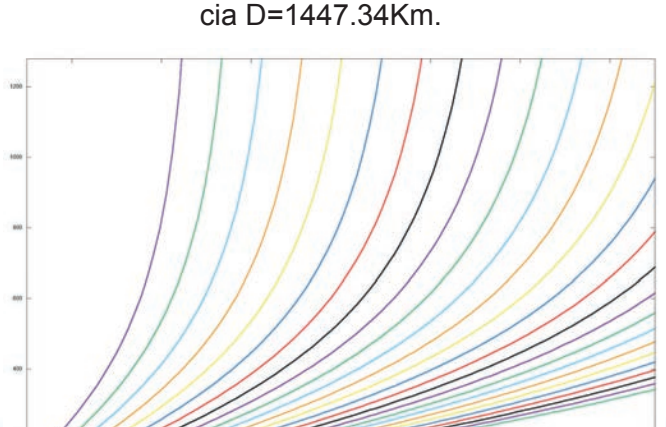
Fonte: DAVIES, K. Ionospheric Radio Propagation. (1965)[1].

A máxima frequência utilizável, a MUF, é o valor máximo de f_{ob} para a distância *D* entre os dois pontos de transmissão. Manipulando a equação para deixarmos em evidência *h'*, teremos

$$h' = \frac{D}{2x\sqrt{\left(\frac{MUF(D)}{kf_v}\right)^2 - 1}}. \qquad (2)$$

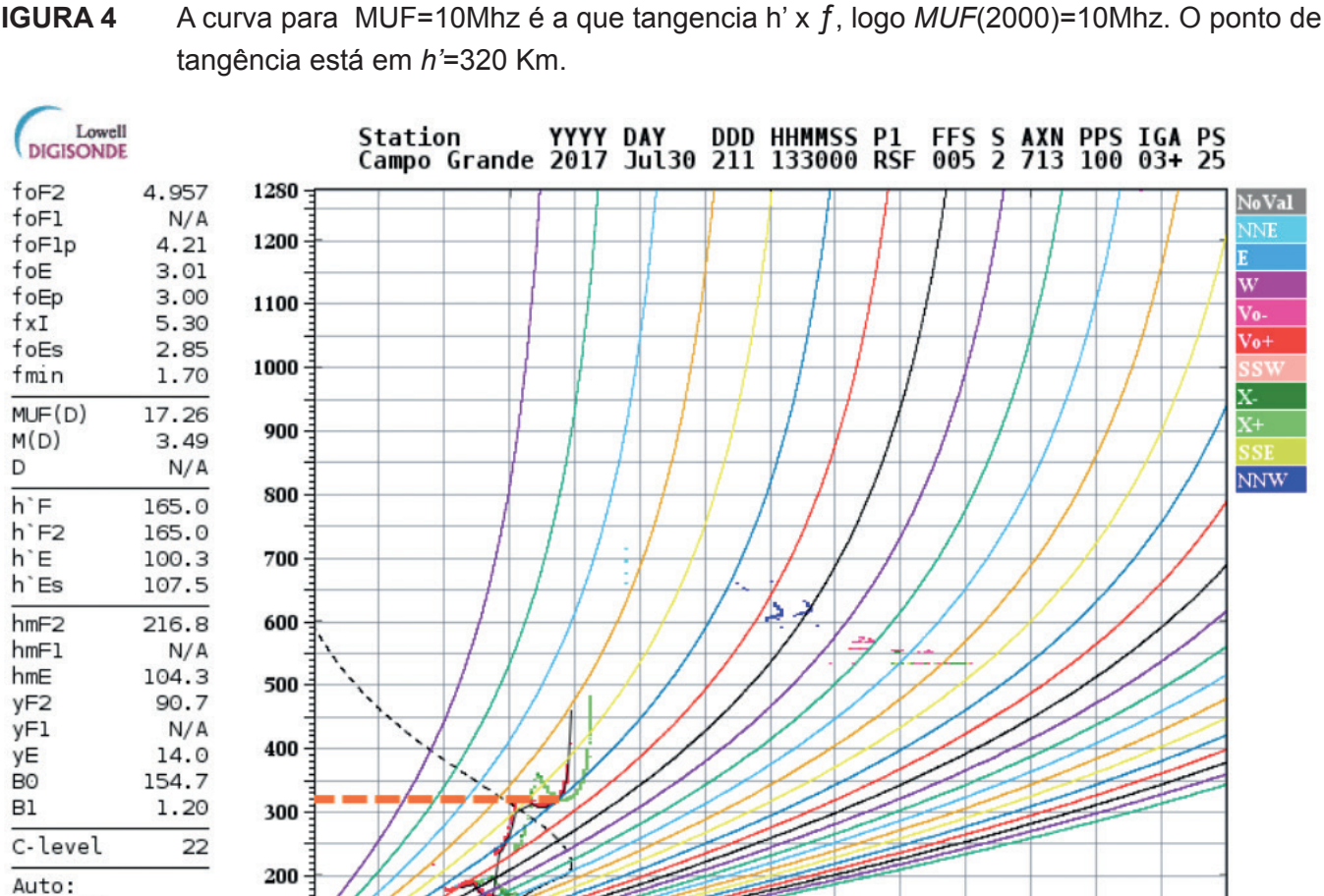
Logo, a partir da distância *D* e do ionograma fornecido podemos obter a *MUF* da transmissão e *h'* para a transmissão de uma forma exata: criamos uma família de curvas (Figura 3) para um dado *D* variando o valor da *MUF* e a sobrepomos sobre o ionograma (Figura 4). O valor certo da *MUF* será o da curva que tangenciar *h' x f*; o valor de *h'* para a frequência da *MUF* será, obviamente, o valor da altura para o ponto encontrado.

FIGURA 3 Família de curvas para uma distância D=1447.34Km.



Fonte: o autor, 2018.

FIGURA 4 A curva para MUF=10Mhz é a que tangencia h' x *f*, logo *MUF*(2000)=10Mhz. O ponto de tangência está em *h'*=320 Km.



Fonte: o autor, 2018.

A partir de análise geométrica simples, conhecendo a altura virtual *h'* determinamos o ângulo de take-off Δ necessário para configurar a antena por meio de

$$\Delta = \tan^{-1}\left(\frac{h' + r\left(1 - \cos\frac{90D}{\pi r}\right)}{r\sin\frac{90D}{\pi r}}\right) - \frac{90D}{\pi r}, \qquad (3)$$

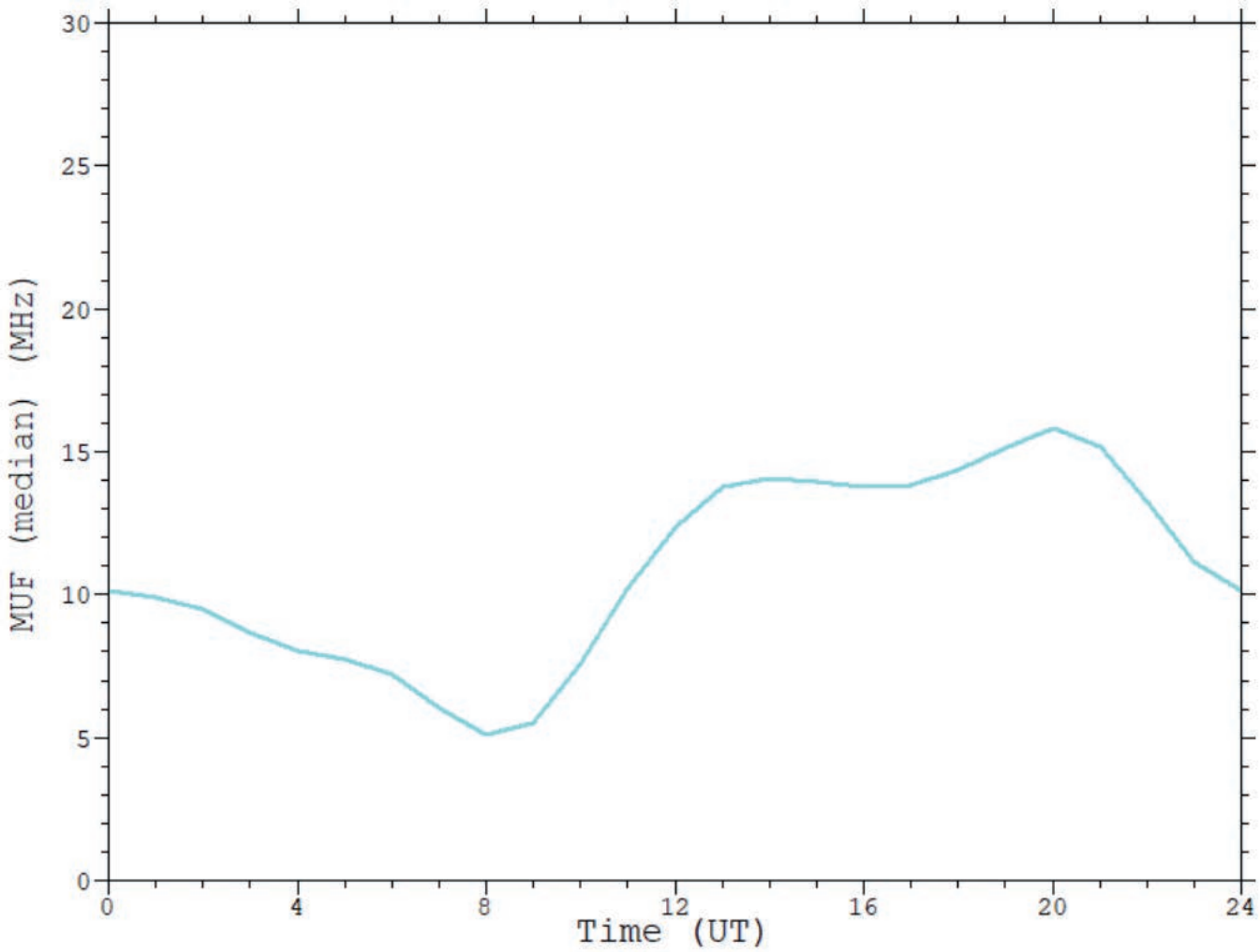
em que *D* é a distância entre os dois pontos de transmissão e *r* é o raio da Terra.

1.2 MÉTODO DAS MÉDIAS MENSAIS

É trabalhoso realizar esta análise gráfica dos ionogramas, que são atualizados a cada dez minutos. Em locais onde seu comportamento é mais previsível e periódico ao longo de um grande período de tempo, como em altas latitudes, costuma-se optar por fazer previsões médias mensais, que sob essas condições são capazes de fornecer com exatidão satisfatória os parâmetros desejados.

Por meio de programas específicos para predição das condições na ionosfera, somos capazes de realizar o cálculo de um valor médio de medidas variadas (como a *MUF* na Figura 5) para um período no tempo longo (de um mês, no mínimo). Eles, no entanto, requerem a inserção de novas variáveis, como o valor médio do número de manchas solares (*SSN*), uma grandeza que pode apresentar grande variância entre dois dias diferentes. Para os cálculos comparativos, foi utilizado o Voice of America Coverage Analysis Program (VOACAP).

FIGURA 5 Previsão para o mês de julho (*SSN*=18) para o valor da *MUF* para uma transmissão entre Brasília, Distrito Federal, e Bela Vista, Mato Grosso do Sul.



Fonte: o autor (2018).

Devido à anomalia de ionização equatorial (EIA), no entanto, o valor da MUF possui grande variância entre os dias de um mesmo mês. Devido a isso, a média mensal entregue por esses métodos pode se mostrar inadequada e subótima.

1.3 MÉTODO COMPUTACIONAL PROPOSTO

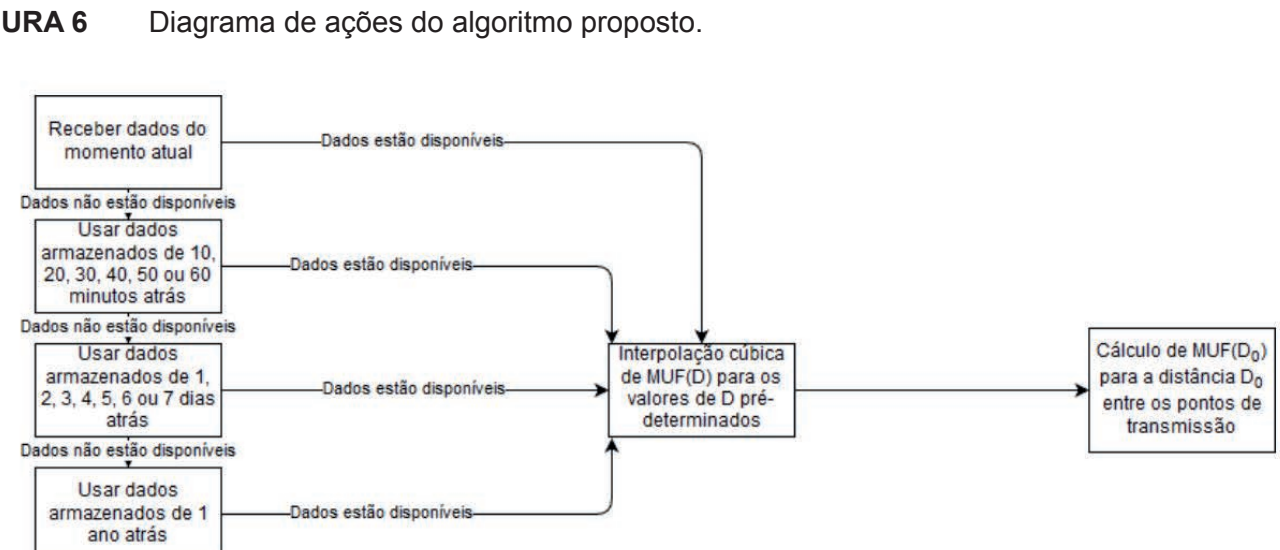
Analisar manualmente os ionogramas vai resultar na solução certa mas é um método custoso e trabalhoso; fazer uso de médias mensais pode-se provar pouco prático quando se há grande variância entre os dias. Propo-

mos, portanto, um método computacional semiautomático que se encarregue de obter automaticamente o valor da *MUF* por meio dos dados fornecidos pelas ionossondas.

O método proposto, como se verifica, é facilmente usado em qualquer ocasião sem os parâmetros adicionais exigidos pelo método das médias mensais. No entanto, assim como a análise manual, exige que haja dados satisfatórios sobre a posição do ponto médio entre as duas pontas da transmissão — certamente, nem sempre vai haver uma ionossonda exatamente neste ponto médio, mas havendo uma perto o suficiente, podemos usar seus dados e aproximá-los como sendo do tal ponto médio.

A ionossonda fornece o valor aproximado de *MUF(D)* para um conjunto pré-determinado de distâncias *D*. A partir de uma interpolação por spline cúbica, podemos obter uma medição razoável para o valor de $MUF(D_0)$, em que D_0=1.147,34 km é a distância entre Brasília e Bela Vista. Não é raro, entretanto, que a ionossonda se encontre inoperante durante períodos extensos de tempo. Neste caso, o algoritmo toma como base os dados de momentos anteriores no tempo, de acordo com a validade da aproximação destes dados com os atuais (Figura 6).

FIGURA 6 Diagrama de ações do algoritmo proposto.



Fonte: o autor, 2017.

1.4 COMPARAÇÃO

Pretendemos comparar a eficiência do algoritmo computacional elaborado com as médias mensais, usando como parâmetro de referência a análise manual dos ionogramas. Para isso, aplicamos as três técnicas anteriormente mencionadas para calcular a *MUF* de uma comunicação entre Brasília e Bela Vista, na região de fronteira do Mato Grosso do Sul com o Paraguai, de forma a simular uma situação real de comunicação do Exército. Dispomos de uma ionossonda de Campo Grande, Mato Grosso do Sul — a cidade se encontra perto o suficiente do ponto médio do caminho entre o ponto de transmissão e o de recepção para considerar que a aproximação é relevante.

Usamos, como amostras, as medições de 9h30 às 19h30, em intervalos de duas horas, de quatro dias diferentes, espaçados por três meses entre si para representarem as quatro estações. Dessa forma, desejamos mostrar o efeito da EIA, cuja intensidade depende da incidência solar e, portanto, do momento do ano, no método das médias mensais.

2 RESULTADOS

Para caráter ilustrativo, tabelamos os valores da *MUF* para uma transmissão entre Brasília, Distrito Federal e Bela Vista, Mato Grosso do Sul (*D*=1.147,34 Km) encontrados por meio da análise manual do ionograma, do cálculo da média mensal por meio do VOACAP e da interpolação dos valores padronizados de *MUF* fornecidos pela ionossondas, junto com as variações relativas *Δ* dos dois últimos métodos em relação ao primeiro método, o de referência. Além disso, calculamos o parâmetro *h'* pelo primeiro e segundo método.

2.1 VERÃO

TABELA 1 Amostras recolhidas para o dia 31 de janeiro de 2017

Hora Local	Ionograma		VOACAP (SSN=26)			Interpolação	
	h'[Km]	MUF(D) [Mhz]	h'[Km]	MUF(D) [Mhz]	*Δ (%)*	MUF(D) [Mhz]	*Δ (%)*
9h30	400	10.0	423	11.6	16.0	9.22	7.8
11h30	600	8.3	492	10.7	28.9	9.70	16.9
13h30	500	12.4	489	11.8	4.8	12.17	1.9
15h30	420	17.8	443	13.7	23.0	16.40	7.9
17h30	390	28.0	400	16.1	42.5	21.90	21.7
19h30	280	16.5	388	15.2	7.9	13.12	20.5

Fonte: o autor, 2018.

2.2 OUTONO

TABELA 2 Amostras recolhidas para o dia 30 de abril de 2017

Hora Local	Ionograma		VOACAP (SSN=32)			Interpolação	
	h'[Km]	MUF(D) [Mhz]	h'[Km]	MUF(D) [Mhz]	*Δ (%)*	MUF(D) [Mhz]	*Δ (%)*
9h30	330	14.0	469	11.3	19.2	11.81	15.6
11h30	310	21.3	505	11.2	47.4	17.47	18.0
13h30	380	17.5	471	12.9	26.3	15.70	10.3
15h30	310	23.3	425	15.2	34.8	19.14	17.9
17h30	300	16.0	395	16.3	1.9	11.65	27.2
19h30	290	8.2	404	14.2	73.2	5.98	27.1

Fonte: o autor, 2018.

2.3 INVERNO

TABELA 3 Amostras recolhidas para o dia 30 de julho de 2017

Hora Local	Ionograma		VOACAP (SSN=18)			Interpolação	
	h'[Km]	MUF(D) [Mhz]	h'[Km]	MUF(D) [Mhz]	*Δ (%)*	MUF(D) [Mhz]	*Δ (%)*
9h30	320	10.0	327	13.8	38	8.36	16.4
11h30	280	12.0	357	13.9	15.8	9.29	22.6
13h30	330	11.0	364	13.8	25.5	9.31	15.4
15h30	290	10.5	351	15.1	43.8	8.37	20.3
17h30	260	11.0	323	15.2	38.2	8.27	24.2
19h30	270	6.3	314	11.1	76.2	4.83	23.3

Fonte: o autor, 2018.

2.4 PRIMAVERA

TABELA 4 Amostras recolhidas para o dia 30 de outubro de 2017

Hora Local	Ionograma		VOACAP (SSN=13)			Interpolação	
	h'[Km]	MUF(D) [Mhz]	h'[Km]	MUF(D) [Mhz]	Δ (%)	MUF(D) [Mhz]	Δ (%)
9h30	340	13.0	362	13.8	6.15	11.13	14.4
11h30	480	12.3	427	13.0	5.7	11.88	3.4
13h30	410	16.6	417	15.0	9.6	15.29	7.9
15h30	340	22.0	390	17.0	22.7	18.73	14.8
17h30	350	20.0	378	19.6	2.0	17.15	14.2
19h30	290	26.0	356	19.6	24.6	20.66	20.5

Fonte: o autor, 2018.

3 DISCUSSÕES

Notamos nos quatro conjuntos de dados que o erro cometido pelo terceiro método é mais estável, poucas vezes ultrapassando a marca de 20% e nunca passando de 30%. Enquanto isso, o do segundo método flutua em demasia — sendo um parâmetro adequado somente para uma análise mensal sem consideração pela grande variância dos valores entre os dias, sua eficácia varia muito. Por vezes, ele é mais certeiro que o método proposto, mas muito frequentemente o erro cometido é demasiado grande, passando várias vezes de 20%.

A *MUF* denota a máxima frequência utilizável — isto é, transmissões realizadas acima dessa frequência não são refletidas pela ionosfera de volta à superfície, e a informação não chega ao seu destino. Somente em uma ocasião o terceiro método retorna uma frequência maior que a de referência, enquanto isto ocorre bastante com o segundo método, revelando um problema crítico deste.

Notamos uma estabilidade do valor da *MUF* no período do inverno, ou seja, quando a incidência solar é menos intensa e a EIA não interfere tanto na transmissão. O terceiro método não é tão eficiente neste período, mas atinge sua maior estabilidade em relação ao erro cometido. O contrário acontece no verão, onde o valor da *MUF* flutua mais — e o erro também.

CONCLUSÕES

Otimizar a frequência de transmissão de forma regular e eficiente é um passo importante na melhoria das comunicações de rádio em alta frequência para a popularização do padrão DRM, que demanda transmissões de alta qualidade, em território nacional. Por ser um padrão digital, ele exige uma taxa de transmissão de dados relativamente grande; saber aumentar essa taxa sem introduzir dano ao sinal é um avanço notável.

O método computacional proposto constitui uma melhoria palpável em relação ao das médias mensais, que, como notamos, é incapaz de lidar com as grandes variâncias entre os dias devido à EIA. Por utilizar dados em tempo real, os resultados do método proposto são pouco afetados pela variância entre os dias; por ser um método automatizado, ele é prático, eficiente e confiável.

É preciso realçar a facilidade proporcionada pela linguagem de programação C++ para implementar o algoritmo proposto. Sua ampla aceitação no meio acadêmico e profissional não só permite a avaliação de pares mas também proporciona, junto ao grande controle que a linguagem dá aos seus usuários, uma enorme gama de livrarias públicas existentes para ela, permitindo mais possibilidades de executar o programa envisionado.

É um desafio, para o futuro, implementar um algoritmo para calcular a altura virtual da atmosfera, algo ainda não atingido pelo método proposto, sendo necessário ainda confiar no método das médias mensais, com todas as

suas falhas, para isto. O ângulo de take-off da antena transmissora é um parâmetro importante para aprimorar a eficiência de potência das transmissões, e é um passo interessante que se desenvolvam soluções nesta direção.

Acreditamos que a viabilização do padrão DRM representa uma nova geração do rádio, com diversas e interessantes aplicações civis e militares, e que a pesquisa contribui de forma fundamental para que estas possibilidades materializem-se em território nacional.

STRATEGIC USE OF IONOSSOND DATA FOR HIGH FREQUENCY (HF) DIGITAL COMMUNICATIONS

Abstract. This project aims to introduce a computational method in order to optimise long-range high frequency radio transmissions. High frequency communication design often employs monthly median ionospheric forecasts that, due to the daytime equatorial ionization anomaly, do not offer great precision at low latitudes, rendering its use in large parts of Brazilian territory unproductive. This initiative seeks to present an alternative procedure so that such a class of communications is made viable in this part of the globe. By using real-time ionosonde data, it is possible to improve the quality of radio transmissions by instantly computing and adjusting its fundamental parameters: its maximum frequency and the antenna's take-off angle. Our work is intended to provide an efficient computational approach, built using C++ and making use of interpolations and graphic analysis of ionograms, in order to estimate these quantities with high accuracy and an algorithm to deal with the ionosonde's long inoperative periods, selecting past data in accordance with the current time of the day and year. By enhancing high frequency radio transmissions, this paper endeavors to develop the viability of the Digital Radio Mondiale (DRM) standard, allowing for secure and inexpensive communication multimedia channels with many strategic military and civilian applications.

Keyword. Digital Radio Mondiale. Radio Transmissions. High Frequency. Ionosonde. C++.

REFERÊNCIAS

DAVIES, Kenneth. **Ionospheric Radio Propagation**. Washington: US Government Printing Office, 1965.

ESTUDO E MONITORAMENTE BRASILEIRO DO CLIMA ESPACIAL. **Ionossondas**. Disponível em: <http://www2.inpe.br/climaespacial/portal/ionossondas-inicio/>. Acesso em: 31 de maio de 2018.

GLOBAL IONOSPHERIC RADIO OBSERVATORY. **Digital Ionogram DataBase**. Disponível em: <http://umlcar.uml.edu/DIDBase/>. Acesso em: 31 de maio de 2018.

Description of the C++ language. Disponível em: <http://www.cplusplus.com/info/description/>. Acesso em: 31 de maio de 2018.

DEITEL, Paul; DEITEL, Harvey. **C++: How to Program**. New Jersey: Pearson Education, 2010.

Vítor Ossamu Rodrigues Okamura é aluno do sétimo semestre de graduação da Universidade de Brasília (UnB) no curso de Engenharia Elétrica. Cursou o ensino médio no Colégio Militar de Brasília (CMB), se formando como 1° Tenente-Aluno. Participou de diversas olimpíadas de conhecimento, conquistando duas medalhas de ouro e duas de bronze na Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP). É fluente em inglês. Pode ser contatado pelo e-mail vitor.ossamu@gmail.com.

Plínio Ricardo Ganime Alves é professor associado 4 do Departamento de Engenharia Elétrica da Universidade de Brasília (UnB). Possui formação em Engenharia Elétrica pelo Instituto Nacional de Telecomunicações (Inatel), mestrado pela Universidade de Brasília (UnB) e doutorado pela Universidade de Limoges. É fluente em inglês e francês. Pode ser contatado pelo e-mail plinio@ene.unb.br.

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

APLICABILIDADE DE INTELIGÊNCIA ARTIFICIAL NOS DISPOSITIVOS DE DEFESA DAS FORÇAS ARMADAS.

Ricardo Rebelo Silva Melo
Pós-graduado em Gestão da Segurança da Informação pela Universidade de Brasília

RESUMO: A Inteligência Artificial (IA) é similiar a inteligência humana, porém com utilização de mecanismo e softwares. A IA vem sendo explorada, com novas experiências e estudos que levam a um patamar conhecido como "agente inteligente". Esse tipo de agente utiliza um conjunto de características para estudar o ambiente e tomar atitudes que maximizam as chances de sucesso em suas decisões. A IA é uma área de pesquisa da computação, que busca métodos ou dispositivos computacionais, que possuam ou multipliquem a capacidade racional do ser humano de resolver problemas, pensar ou, de forma ampla, ser inteligente. Comumente definida como o ramo da ciência da computação que se ocupa do comportamento inteligente, capacidade de fazer os computadores realizarem coisas que, atualmente, os humanos fazem melhor. O sistema de IA deve ter um pensamento diferenciado, capaz de possibilitar às máquinas realizarem trabalhos superiores ao do raciocínio humano. Para isso, o sistema trabalha sinergicamente a capacidade de raciocínio, aprendizagem, reconhecimento padrão e inferência. A capacidade de raciocínio trabalha as regras lógicas para se chegar a uma conclusão o mais rápido possível. A aprendizagem sistematiza a compreensão dos erros e acertos armazenados em um banco de dados. O reconhecimento padrão é o visual, sensorial e de comportamento, superior ao do ser humano. E, por fim, a inferência é a aplicação do raciocínio nas situações do cotidiano. Esse agente inteligente é capaz de potencializar drasticamente a eficiência do emprego de tropas militares num cenário a médio prazo, havendo necessidade de ampliar as pesquisas nessa área.

Palavras-chave: Inteligência artificial. Uniformes. Armamentos individuais.

O Exército Brasileiro (EB) encontra-se em um processo de evolução tecnológica em suas Armas (Infantaria, Comunicação, Artilharia, Cavalaria e Engenharia), para o constante aperfeiçoamento da Força Terrestre, tornando-se mais eficiente.

A pesquisa sobre Inteligência Artificial (IA) começou após a Segunda Guerra Mundial, mas atualmente é aplicada em vários setores empresariais, desde jogos até a manipulação de carros sem motoristas. De acordo com a explicação e a Tabela 1 do autor Russell, é possível visualizar a forma como é o pensamento humano e o pensamento racional, e como o ser humano age e o agir racional:

Em linhas gerais, as que estão na parte superior da tabela se relacionam a processos de pensamento e raciocínio, enquanto as definições da parte inferior se referem ao comportamento. As definições do lado esquerdo medem o sucesso em termos de fidelidade ao desempenho humano, enquanto as definições do lado direito medem o sucesso comparando-o a um conceito ideal de inteligência, chamado de racionalidade. (RUSSELL, 2013).

TABELA 1 Pensamento humano e pensamento racional.

Pensando como um humano	Pensando racionalmente
O novo e interesante esforço para fazer os computadores pensarem (...) máquinas com mentes, no sentido total e literal. (HAUGELAND, 1985). [Automação de] atividades que associamos ao pensamento humano, atividades como a tomada de decisões, a resolução de problemas, o aprendizado(...) (BELLMAN, 1978).	O estudo das faculdades mentais pelo uso de modelos computacionais (CHARNIAK e MCDERMOTT, 1985). O estudo das computações que tornam possíveis perceber, raciocinar e agir (WINSTON, 1992).

Agindo como seres humanos	Agindo racionalmente
A arte de criar máquinas que executam funções que exigem inteligência quando executadas por pessoas. (BELLMAN, 1978). O estudo de como os computadores podem fazer tarefas que hoje são melhor desempenhadas pelas pessoas (RICH & KNIGHT, 1991).	Inteligência Computacional é o estudo do projeto de agentes inteligentes (POOLE et al, 1998). AI ... está relacionada a um desempenho inteligente de artefatos. (NILSSON, 1998).

Fonte: Russell, 2013.

O teste de Turing, proposto pelo pai da ciência da computação, Alan Turing, consiste em uma máquina realizar uma conversa com o interrogado durante cinco minutos. Durante esse tempo o interrogador deve adivinhar se a conversa que teve foi através de um computador ou uma pessoa. O programa passa no teste se enganar o interrogador por 30% do tempo. Sendo assim, muitas pessoas conseguiram ser enganadas. Um dos programas utilizados foram ELIZA e os chatbots da Internet chamados: MGONZ, NATACHATA e CYBERLOVER. Portanto, o computador para passar no teste necessita de um programa avançado e com as seguintes capacidades, segundo Alan Turing:

> • processamento de linguagem natural para permitir que ele se comunique com sucesso em um idioma natural;
>
> • representação de conhecimento para armazenar o que sabe ou ouve;
>
> • raciocínio automatizado para usar as informações armazenadas com a finalidade de responder a perguntas e tirar novas conclusões;
>
> • aprendizado de máquina para se adaptar a novas circunstâncias e para detectar e extrapolar padrões. (RUSSELL, 2013).

O teste de Turing não necessita da intervenção física entre o ser humano e computador. Isto não tem importância para o estudo de inteligência. Do total, são necessárias as inclusões de sinais de vídeos, para que o interrogador possa testar as habilidades de percepção do indivíduo. Sendo assim, o computador necessita também das seguintes características, de acordo com o pai da ciência da computação:

> • visão computacional para perceber objetos; e
>
> • robótica para manipular objetos e movimentar-se. (RUSSELL, 2013).

Seguindo por essas caracterísitcas citadas, verifica-se a evolução de várias tecnologias baseadas na IA, como na área de defesa e ataque das Forças Armadas. Uma forma de evoluir nos meios de guerra, principamente na linha de frente como os soldados, seria a implantação de IA nos uniformes e armamentos individuais trazendo consigo uma nova evolução de combate aos territórios brasileiros.

1 METODOLOGIA

O problema levantado surgiu em um projeto de hackthon, ao analisar como os militares se comportam para realizar um tipo de manobra de invasão em um território hostil. A pesquisa foi executada de forma qualitativa, estudando particulamente o tema abordado, buscando tendências, pensamentos ou opiniões acerca do tema, com observações.

A pesquisa tem uma tendência de natureza exploratória, uma vez que se buscou criar um novo pensamento sobre utilização de tecnologia com IA. Essa pesquisa está sendo elaborada para criar ideias que possibilitem uma aplicação futura em novos estudos por parte de outros pesquisadores com conhecimento aprofundado em IA.

O trabalho foi realizado através de uma pesquisa bibliográfica e, após uma leitura analítica dos artigos e das literatura selecionadas, chegou-se à conclusão desejada.

A pesquisa não levou em consideração a existência de organizações militares que conduzam pesquisas de inteligência artificial ou implantação de tecnologia de melhorias nos meios de combate do Exército, inviabilizando o emprego de outros instrumentos como entre-

vistas ou questionários.

Há vasta literatura sobre inteligência artificial, mas muito pouco sobre implantação dessa tecnologia em meios de combate nas Forças Armadas ou nas forças auxiliares.

Sendo assim, este artigo faz exatamente essa ligação, da implantação da inteligência artificial nos meios de combate, como uniforme e armamento individual dos militares do Exército.

Novos estudos e pesquisas de outras implantações de IA no ambiente de defesa do Exército devem ser realizados.

2 RESULTADOS E DISCUSSÕES

2.1 INTELIGÊNCIA ARTIFICIAL E O EXÉRCITO BRASILEIRO

O Exército Brasileito está passando por uma transformação ímpar, que atinge ensino, doutrina, tecnologias e organizações militares, preparando-se para atuar em prol de suas missões constitucionais com eficácia e eficiência.

Fatos como a criação do Centro de Defesa Cibernética, em 2010, e ativação em 2012, lançam novos e empreendedores desafios ao Exército. Já é possível questionar: quais serão as necessidades do “Soldado do futuro”? E, ainda, quais meios estarão a sua disposição?

Um Exército em plena transformação é capaz de vislumbrar as tendências e se lançar a novos horizontes. Não, apenas, proteger sistemas, infraestrturas e neutralizar fontes de ataque. É possível ir além!

Há algumas décadas, a EsCom ministrava apenas conhecimentos na área de radiocomunicação, telegrafia e sinaleiro. Hoje, a Escola ministra conhecimentos avançados em rede de computadores, proteção cibernética, smat grid, sistemas de automação inteligentes, acompanhando as tendências e desenvolvendo pesquisas nas áreas de conhecimento afetos à Defesa Nacional.

O presente cenário é propício ao desenvolvimento de estudos interligados a IA. De maneira simples, visualiza-se ensaios na implantação da IA em uniformes e armamentos individuais.

2.2 A INTELIGÊNCIA ARTIFICIAL: PRINCIPAIS CONCEITOS E SUAS IMPLANTAÇÕES.

A inteligência artificial, como mencionado anteriormente, é baseada em estudos na área da informática para criar máquinas inteligentes, ou seja, máquinas com velocidade de pensamento mais rápido ou até melhor que o pensamento humano. Ela serve para analisar todas as possibilidades que podem ocorrer um determinado problema para que seja resolvido de forma mais rápida e correta. Com isso, a IA possui algumas propriedades no ambiente de tarefa. De acordo com Russell:

> • **Completamente observável versus parcialmente observável**: Se os sensores de um agente permitem acesso ao estado completo do ambiente em cada instante, dizemos que o ambiente de tarefa é completamente observável. Um ambiente de tarefa é de fato completamente observável se os sensores detectam todos os aspectos que são relevantes para a escolha da ação; por sua vez, a relevância depende da medida de desempenho. Ambientes completamente observáveis são convenientes porque o agente não precisa manter qualquer estado interno para acompanhar as mudanças do mundo. Um ambiente poderia ser parcialmente observável devido ao ruído e a sensores imprecisos ou porque partes do estado estão simplesmente ausentes nos dados do sensor. Se o agente não tiver sensores, o ambiente será inobservável.
>
> • **Agente único versus multiagente**: A distinção entre ambientes de agente único e de multiagente pode parecer bastante simples. Por exemplo, um agente que resolve um jogo de palavras cruzadas sozinho está claramente em um ambiente de agente único, enquanto um agente que joga xadrez está em um ambiente de dois agentes.
>
> • **Determinístico versus estocásti-**

co: Se o próximo estado do ambiente é completamente determinado pelo estado atual e pela ação executada pelo agente, dizemos que o ambiente é determinístico; caso contrário, ele é estocástico. Em princípio, um agente não precisa se preocupar com a incerteza em um ambiente completamente observável e determinístico. Porém, se o ambiente for parcialmente observável, ele poderá parecer estocástico. A maioria das situações reais é tão complexa que é impossível acompanhar todos os aspectos não observados; para finalidades práticas devem ser tratados como estocásticos.

• **Episódico versus sequencial**: Em um ambiente de tarefa episódico, a experiência do agente é dividida em episódios atômicos. Em cada episódio, o agente recebe uma percepção e em seguida executa uma única ação. É crucial que o episódio seguinte não dependa das ações executadas em episódios anteriores. Em ambientes episódicos, a escolha da ação em cada episódio só depende do próprio episódio. Por outro lado, em ambientes sequenciais, a decisão atual poderia afetar todas as decisões futuras. Ambientes episódicos são muito mais simples que ambientes sequenciais porque o agente não precisa pensar à frente.

• **Estático versus dinâmico**: Se o ambiente puder se alterar enquanto um agente está deliberando, dizemos que o ambiente é dinâmico para esse agente; caso contrário, ele é estático. Ambientes estáticos são fáceis de manipular porque o agente não precisa continuar a observar o mundo enquanto está decidindo sobre a realização de uma ação nem precisa se preocupar com a passagem do tempo. Por outro lado, ambientes dinâmicos estão continuamente perguntando ao agente o que ele deseja fazer; se ele ainda não tiver se decidido, isso será considerado a decisão de não fazer nada. Se o próprio ambiente não mudar com a passagem do tempo, mas o nível de desempenho do agente se alterar, diremos que o ambiente é semidinâmico.

• **Discreto versus contínuo**: A distinção entre discreto e contínuo aplica-se ao estado do ambiente, ao modo como o tempo é tratado, e ainda às percepções e ações do agente.

• **Conhecido versus desconhecido**: Estritamente falando, essa distinção não se refere ao ambiente em si, mas ao estado de conhecimento do agente (ou do projetista) sobre as “leis da física” no meio ambiente. Em um ambiente conhecido, são fornecidas as saídas (ou probabilidades das saídas se o ambiente for estocástico) para todas as ações. Obviamente, se o ambiente for desconhecido, o agente terá de aprender como funciona, a fim de tomar boas decisões. (RUSSELL, 2013).

A tabela 2 mostra como seria a implantação das propiedades da IA no Uniformes e armamentos individuais do militares. Esses estudo foi realizado conforme o conceito explicativo de cada termo da propriedade da Inteligência Artificial.

TABELA 2 Utilização da propriedade da IA para os uniformes e armamentos individuais dos militares.

AMBIENTE	OBSERVÁVEL	AGENTES	DETERMINÍSTICO	EPISÓDICO	ESTÁTICO	DISCRETO
UNIFORME	PARCIALMENTE	MULTI	ESTOCÁCIO	EPISÓDICO	DINÂMICO	DISCRETO
ARMAMENTO INDIVIDUAL	PARCIALMENTE	MULTI	ESTOCÁCIO	EPISÓDICO	DINÂMICO	DISCRETO

Fonte: o autor.

O comportamento realizado até agora refere-se aos agentes através de suas ações executadas após uma sequência de percepções específicas de suas propriedades.

A IA tem como objetivo projetar o programa do agente, que tem como tarefa implementar função de percepções do agente. O agente é formado pela arquitetura e programa, segundo Russell:

> Agente = arquitetura + programa. (RUSSELL, 2013).

A arquitetura é formada por dispositivos de computadores com sensores e atuadores físicos. E os programas devem ser apropriados

e compatíveis para a arquitetura utilizada.

No caso dos uniformes, o programa deve incluir movimentos de caminhadas, corridas, agachamentos, rotação dos braços, abertura e fechamento das mãos, braços e pernas. Então a arquitetura deve incluir braços, mãos e pernas.

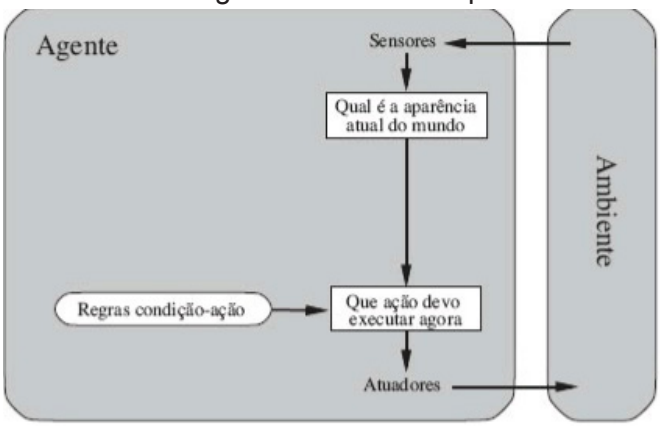
Os programas de agentes tem como uma das caraterísitcas receber uma percepção atual como entrada no sensores e depois de realizar essa leitura devolver como uma ação para os atuadores.

O programa de agente é diferente da funções do agente. Enquanto o programa de agente se preocupa apenas com a percepção atual como entrada, a função do agente se preocupa com o histórico recebido para as percepções completas.

Existem quatro tipos básicos de programas de agente que são, segundo Russell:

• **Agentes reativos simple**s – agente selecionam ações com base na percepção atual, ignorando o restante do histórico de percepções. A figura 2.2.1 mostra o diagrama esquemático de um agente reativo simples. (RUSSELL, 2013).

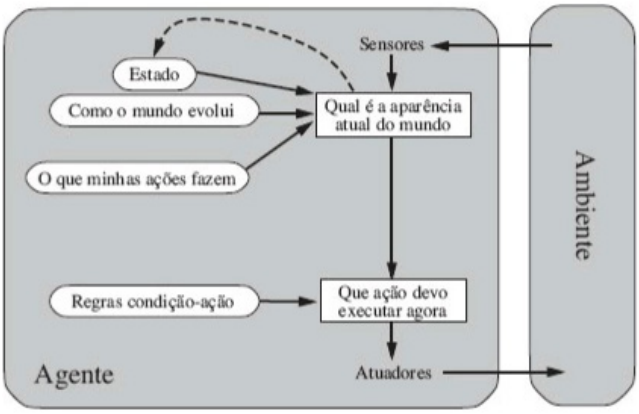
FIGURA 2.2.1 Agentes reativos simples



Fonte: (Russell, 2013).

• Agentes reativos baseados em modelo - O modo mais efetivo de lidar com a possibilidade de observação parcial é o agente monitorar a parte do mundo que ele não pode ver agora. Isto é, o agente deve manter algum tipo de estado interno que dependa do histórico de percepções e assim reflita pelo menos alguns dos aspectos não observados do estado atual. A figura 2.2.2 mostra o agente reativo baseado em modelo. (RUSSELL, 2013).

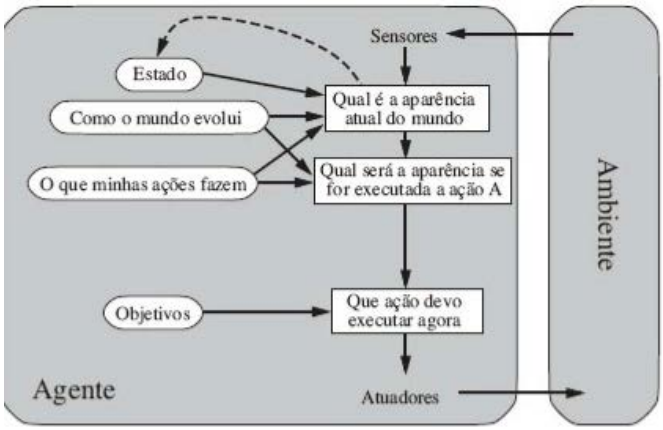
FIGURA 2.2.2 Agentes reativos baseados em modelos



Fonte: (Russell, 2013).

• Agentes baseados em objetivos – Uma atividade que deve tomar decisões de acordo com o objetivo apresentado, ou seja, tomar decisões para alcançar o objetivo determinado. A figura 2.2.3 mostra o agente baseado em objetivos. (RUSSELL, 2013).

FIGURA 2.2.3 Agentes baseados em objetos



Fonte: (Russell, 2013).

• Agentes baseados na utilidade – Essa atitude deve ser baseado no objetivo a ser alcançado de forma de forma com alta qualidade no ambiente, de forma mais segura, rápida, eficiente, confiável e mais econômica, por isso chamado de utilidade. A figura 2.2.4 mostra o agente baseado em utilidade. (RUSSELL, 2013).

FIGURA 2.2.4 Agentes baseados na utilidade

Fonte: (Russell, 2013).

A IA possui vários recursos de agentes a ser implementados, por isso ao analisar cada um de seus agentes, deve se tomar uma decisão baseada nas necessidades de cada atividade ou regras de tomadas de decisões a ser implementa juntamente com suas características.

2.3 APLICABILIDADE DA INTELIGÊNCIA ARTIFICAL NOS UNIFORMES E ARMAMENTO INDIVIDUAL

De acordo com a teoria dos agentes e as características da Inteligência Artificial, uniformes e armamentos individuais, poderiam ser revestidos de tecnologia que auxiliassem os combatentes nas tomadas de decisão. Poucas linhas de programação seriam suficientes para habilitar sensores a análise de vulnerabilidades do meio ambiente em que o militar se encontra, identificação do posicionamento da tropa, eixos de deslocamento, prospecção 3D do terreno, identificação da posição de deflagação do tiro inimigo, direção de tiro, condições do terreno, estado de saúde, estado mental. É possível implementar, inclusive, coleta e armazenamento de dados, para fins diversos. Há uma diversidade de informações que podem ser colhidas ou prestadas, pelo emprego de sensores nos uniformes e nos armamentos ampliando o poder de combate do indivíduo e do grupo.

CONCLUSÕES

O presente estudo caracteriza os conceitos afetos a IA e, exemplifica, por intermédio da implantação de sensores em vestuário e armamento, algumas possibilidades de emprego. Concomitantemente, evidencia-se premência de novos e mais aprofundados estudos na temática, englobando, inclusive, a manipulação e criação de programas e arquiteturas que se amoldem as necessidades da Força Terrestre.

O país possui pesquisadores de renome imersos no meio acadêmico, além de uma indústria em constante interação com o setor acadêmico no desenvolvimento de tecnologia de ponta. A recente aproximação do Exército com a Indústria e a Academia viabilizam pesquisas em IA, que objetivem resolver problemas e ampliar capacidades operacionais.

Na opinião deste autor, há amplo emprego para a tecnologia de IA em prol do Exército Brasileiro. No entanto, sua implementação deve analisar, também, as vulnerabilidades da tecnologia e mecanismos de proteção que viabilizem seu uso.

APPLICABILITY OF ARTIFICIAL INTELLIGENCE IN ARMED FORCES DEFENSE DEVICES

ABSTRACT. ARTIFICIAL INTELLIGENCE (AI) IS SIMILAR TO HUMAN INTELLIGENCE, BUT WITH THE USE OF MECHANISM AND SOFTWARE. THE AI HAS BEEN EXPLORED, WITH NEW EXPERIENCES AND STUDIES THAT LEAD TO A LEVEL KNOWN AS "INTELLIGENT AGENT". THIS TYPE OF AGENT USES A SET OF CHARACTERISTICS TO STUDY THE ENVIRONMENT AND TAKE ACTIONS THAT MAXIMIZE THE CHANCES OF SUCCESS IN THEIR DECISIONS.

AI IS AN AREA OF COMPUTATIONAL RESEARCH THAT SEEKS COMPUTATIONAL METHODS OR DEVICES THAT POSSESS OR MULTIPLY THE RATIONAL CAPACITY OF THE HUMAN BEING TO SOLVE PROBLEMS, TO THINK OR TO BE INTELLIGENT. COMMONLY DEFINED AS THE BRANCH OF COMPUTER SCIENCE THAT DEALS WITH INTELLIGENT BEHAVIOR, THE ABILITY TO MAKE COMPUTERS PERFORM THINGS THAT HUMANS DO BEST TODAY. THE AI SYSTEM MUST HAVE A DIFFERENTIATED THINKING, CAPABLE OF ALLOWING THE MACHINES TO PERFORM WORK SUPERIOR TO THAT OF HUMAN REASONING. TO DO THIS, THE SYSTEM WORKS SYNERGISTICALLY WITH REASONING, LEARNING, STANDARD RECOGNITION, AND INFERENCE. THE REASONING ABILITY WORKS THE LOGICAL RULES TO COME TO A CONCLUSION AS QUICKLY AS POSSIBLE. LEARNING SYSTEMATIZES THE UNDERSTANDING OF ERRORS AND HITS STORED IN A DATABASE. THE STANDARD RECOGNITION IS THE VISUAL, SENSORY AND BEHAVIOR, SUPERIOR TO THAT OF THE HUMAN BEING. AND, FINALLY, INFERENCE IS THE

APPLICATION OF REASONING IN EVERYDAY SITUATIONS. THIS INTELLIGENT AGENT IS CAPABLE OF DRASTICALLY ENHANCING THE EFFICIENCY OF THE USE OF MILITARY TROOPS IN A MEDIUM-TERM SCENARIO, ENABLING MORE RESEARCH IN THIS AREA OF KNOWLEDGE.

KEYWORDS: ARTIFICIAL INTELLIGENCE. UNIFORMS. INDIVIDUAL ARMAMENTS.

REFERÊNCIAS

CDCIBER, Centro de Defesa Cibernética. Disponível em: <https://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cedn/viii_cedn/cibercidviiicedn.pdf> Acesso em: 22 julho 2018.

EPEx. Escritório de Projetos do Exército Brasileiro. Disponível em: < http://www.epex.eb.mil.br/index.php/defesa-cibernetica/defesa-cibernetica> Acesso em 22 julho 2018

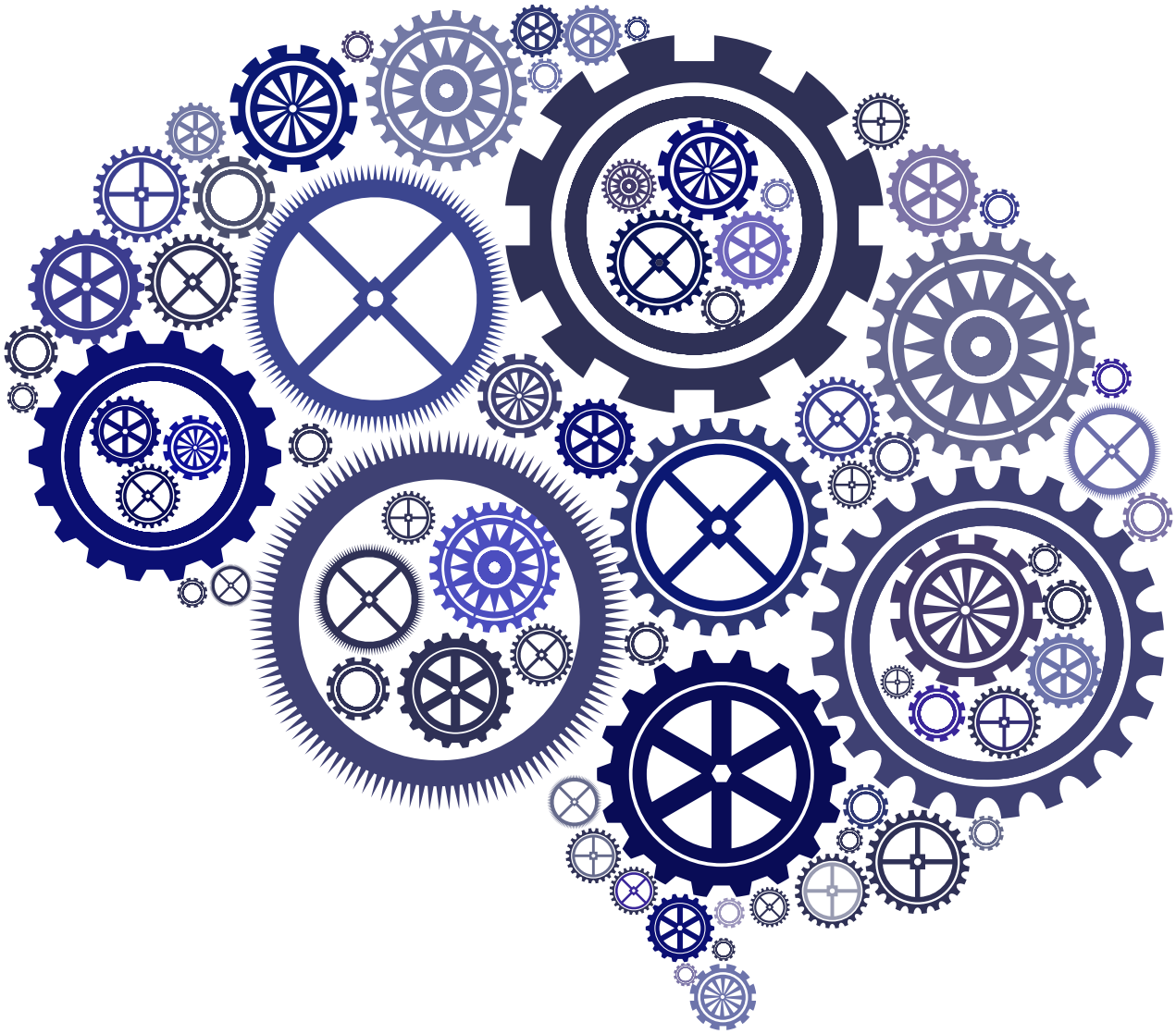
Escola de Comunicações, Disponível em: <http://www.escom.eb.mil.br/historico> Acesso em 22 julho 2018.

GUNKEL, David J. Comunicação e inteligência artificial: novos desafios e oportunidades para a pesquisa em comunicação. 2016. Professor da Northern Ilinois University (USA).

MAGNU, Thiago. Entenda o que é Inteligência Artificial e como ela pode mudar tudo o que conhecemos.TD, Disponível <https://transformacaodigital.com/o-que-e-inteligencia-artificial/> Acesso em 22 julho 2018.

RUSSELL, Stuart J.Russell, Stuart J. (Stuart Jonathan), 1962-Inteligência artificial / Stuart Russell, Peter Norvig; tradução Regina Célia Simille. – Rio de Janeiro: Elsevier, 2013.

O autor é bacharel em Engenharia de Computação pelo Centro Universitário de Brasília (UniCeub). Possui especialização em Gestão de Segurança da Informação pela Universidade de Brasília (UnB) e pode ser contatado pelo e-mail ricardorebelomelo@gmail.com.



CICAD.I.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

SEGURANÇA CIBERNÉTICA: O OLHAR DA DEFESA NACIONAL E DA INTELIGÊNCIA DE ESTADO FRENTE ÀS VULNERABILIDADES DIGITAIS

Alexsandro Barreto Gois
Mestrando em Economia da Defesa pela Universidade de Brasília

RESUMO: O presente artigo trata sobre a segurança cibernética, um paradigma atual que está gerando uma crescente preocupação de entidades públicas e privadas em todo o mundo. Antigamente as ameaças eram, em sua grande maioria, visíveis e tangíveis. Mas, com o avanço das tecnologias de comunicação e informação, isso mudou. As ameaças atuais estão invadindo os sistemas eletrônicos das corporações, prejudicando suas atividades. Diante disso, surgem preocupações para uma nova forma de segurança e proteção frente às vulnerabilidades digitais: segurança cibernética. A segurança cibernética é uma preocupação atual e crescente de diversas instituições, tanto públicas quanto privadas. A preocupação é latente e já está normatizada nas políticas públicas de instituições de segurança pública, como é evidente nas Estratégias Nacional de Defesa e Nacional de Inteligência. Neste artigo, demonstra-se essa normatização e consequente preocupação, tanto da área de Defesa quanto da área de Inteligência. Ainda, comenta-se casos de ataques cibernéticos que ocorreram em algumas instituições públicas e privadas. A preocupação com uma nova forma de defesa é necessária para as instituições que trabalham com segurança. Como salvaguardar os sites e sistemas de suas instituições? É possível se defender desses tipos de ataques, ou estamos à mercê dos ataques cibernéticos?

Palavras-chave: Segurança cibernética. Vulnerabilidades digitais. Defesa Nacional. Estratégia Nacional de Defesa. Estratégia Nacional de Inteligência.

INTRODUÇÃO

Recentemente, uma sequência de ataques cibernéticos tem acometido diversas instituições, causando transtornos e prejuízos de grande soma. Por isso, o propósito deste artigo é analisar o olhar dos órgãos que se preocupam com Segurança Cibernética, como a Defesa Nacional e a Inteligência de Estado, tendo em vista as vulnerabilidades digitais existentes.

O fato de o Brasil ser um dos países que lidera o ranking de ataques cibernéticos, provoca grandes discussões sobre o aparato de proteção contra eles. A indagação de o Brasil estar preparado para a Defesa Cibernética é uma discussão feita neste trabalho.

Para responder a essa indagação, necessário se faz analisar a normatização estratégica de duas áreas de segurança: a Defesa Nacional e a Inteligência de Estado. Ambas demonstram, em suas Estratégias Nacionais, a preocupação com os ataques cibernéticos e propõem, em sentido similar, a capacitação de seu corpo técnico com conhecimentos e habilidades que auxiliem no combate ao crime em ambiente virtual.

1 SEGURANÇA CIBERNÉTICA

Considerando os atuais avanços das Tecnologias da Informação e Comunicação (TIC), foi constatado, pela presença cada vez maior de tecnologias no cotidiano da sociedade, o elevado uso de smartphones, tablets, relógios digitais, computadores, dentre outros equipamentos. Os quais fornecem acesso à internet, possibilitando a realização de trabalhos remotos, transações financeiras, ensino a distância (EaD), utilização de redes sociais,

disponibilização de documentos, fotos e vídeos na "nuvem" ou disponíveis para acesso sem restrições de usuários etc. Tudo disponível em um único clique, acessível a tudo e a todos.

Entretanto, isso requer cuidado, preocupação e medidas de segurança dos usuários das TIC. Tendo em vista essa preocupação, Canongia e Mandarino Júnior (2009) revelam que um dos grandes receios da atualidade é com a segurança no mundo digital. É evidente que a abertura de dados e a disponibilização de informações de forma ostensiva proporcionam fragilidades quanto à segurança de dados e informações.

Nesse sentido, seguindo as palavras de Mandarino Júnior (2009), que define segurança cibernética como 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. Devemos nos preocupar com a segurança cibernética, reduzindo ao máximo vulnerabilidades disponíveis na rede mundial de computadores. Mas, como podemos nos proteger disso? Nós, como cidadãos, temos as "armas" necessárias para essa defesa? O Estado pode nos ajudar? A Segurança Pública se preocupa com essa nova forma de Defesa? As Forças Armadas também se preocupam com a segurança da informação? A Atividade de Inteligência reconhece essa fragilidade como uma ameaça a ser observada? Essas indagações são recorrentes e este artigo se propõe a respondê-las.

É crescente o cuidado dos governos em salvaguardar seus bancos de dados, com o fim de evitar cibercrimes, e em desenvolver e capacitar o seu corpo técnico para lidar com questões de segurança de dados e de informações (CANONGIA e MANDARINO JÚNIOR, 2009). Assim, considerando o elevado compartilhamento de dados e informações nas redes sociais, o aumento do armazenamento em "nuvens" e a importância das informações arquivadas em computadores, as questões ligadas à segurança, privacidade e confidencialidade tornam-se essenciais para a proteção de dados e de informações.

Nesse contexto, a segurança cibernética é uma preocupação global que objetiva assegurar ao máximo a disponibilidade, confidencialidade, integridade e autenticidade de dados e informações, haja vista a formulação de estratégias para o processo decisório nacional (CANONGIA e MANDARINO JÚNIOR, 2009). Além dos Estados, as organizações do setor privado e as pessoas físicas também estão preocupadas com a proteção de seus dados e informações, situação que cresce à proporção que se expande o número de usuários das TIC.

Por esse motivo, é importante a normatização de ações voltadas à Segurança Cibernética e à adoção de políticas públicas para essa área. Assim, a partir desse momento, iremos analisar as normas que estão voltadas a ações de proteção e salvaguarda contra ataques cibernéticos, que estão expressas na Estratégia Nacional de Defesa (END) e na Estratégia Nacional de Inteligência (Enint).

1.1 ESTRATÉGIA NACIONAL DE DEFESA

A END tem como propósito estabelecer diretrizes para a adequada preparação e capacitação das Forças Armadas, possibilitando a garantia da segurança do país em diversos cenários, tanto em tempo de paz quanto em situações de conflito. Uma congruente estrutura de defesa assegura maior estabilidade ao país e proporciona a devida proteção de seu território, de sua população e de setores considerados estratégicos da economia.

Esse documento definiu ações estratégicas num espectro de médio e longo prazos, objetivando a modernização da estrutura nacional de defesa. Dedica-se, também, a questões político-institucionais que assegurem os meios para fazer com que o governo e a sociedade empreguem decisivamente os conceitos inerentes à estratégia de segurança nacional. Além, é claro, de tecer temas propriamente militares, fixando orientações e paradigmas para

a atuação operacional do Exército, da Marinha e da Aeronáutica.

A referida estratégia foi estruturada em quatro eixos principais, os quais abordam: a) como as Forças Armadas devem se organizar e se orientar para melhor desempenharem sua destinação constitucional e suas atribuições na paz e na guerra; b) a reorganização da Base Industrial de Defesa, para assegurar o atendimento às necessidades de equipamentos das Forças Armadas apoiado em tecnologias sob domínio nacional, preferencialmente as de emprego dual (militar e civil); c) composição dos efetivos das Forças Armadas; d) o futuro do serviço militar obrigatório, observando a necessidade das Forças Armadas serem constituídas por cidadãos oriundos de todas as classes sociais.

Ainda, enumerou vinte e cinco diretrizes para nortear as distintas áreas de preocupação, com o fim de desenvolver ações estratégicas da Defesa Nacional. Dentre elas, a sexta diretriz pauta-se no fortalecimento de três setores de importância estratégica, quais sejam: o espacial, o cibernético e o nuclear.

O setor cibernético, que faz parte do escopo deste trabalho, se preocupa como as capacitações se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Integrarão, como prioridade, as TIC entre todos os agrupamentos das Forças Armadas, de modo a assegurar sua capacidade para atuar em rede. As prioridades do setor cibernético elencadas na END são as seguintes:

a) fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas;

b) aprimorar a Segurança da Informação e Comunicações (SIC), particularmente, no tocante à certificação digital no contexto da Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa), integrando as ICP das três Forças;

c) fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional. Nesse contexto, os Ministérios da Defesa, da Fazenda, da Ciência, Tecnologia e Inovação, da Educação, do Planejamento, Orçamento e Gestão, a Secretaria de Assuntos Estratégicos da Presidência da República e o Gabinete de Segurança Institucional da Presidência da República deverão elaborar estudo com vistas à criação da Escola Nacional de Defesa Cibernética;

d) desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual;

e) desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional, tais como sistema modular de defesa cibernética e sistema de segurança em ambientes computacionais;

f) desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas;

g) incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas; e

h) estruturar a produção de conhecimento oriundo da fonte cibernética. (BRASIL, 2012).

As prioridades do setor cibernético citadas acima demonstram o norte de atuação das ações que as Forças Armadas devem dispensar para assegurar a defesa nesse setor. Das oito prioridades, percebe-se que é latente a preocupação com o fortalecimento, aprimoramento, desenvolvimento e capacitação por meio de conhecimentos, estudos e tecnologias que fomentem o fortalecimento dessa área. Nessa linha de raciocínio, Carvalho et al (2006) comentam a importância na capacitação em pesquisa e desenvolvimento:

A manutenção da soberania nacional implica, basicamente, na capacitação em pesquisa e no desenvolvi-

> mento dos recursos humanos para que eles sejam capazes de contribuir com soluções organizacionais e tecnológicas específicas. Às vezes, torna-se necessária a geração do conhecimento por meio de importação de "pacotes tecnológicos" a serem posteriormente "abertos", adaptados às necessidades da instituição e otimizados por "engenharia reversa".

A pesquisa e desenvolvimento dos recursos humanos no setor cibernético são imprescindíveis, nos dias atuais, para promover a proteção do Estado, da sociedade e dos setores estratégicos da economia, com o intuito de capacitá-los com soluções e tecnologias recentes. Isso demonstra o valor de expressar na END a preocupação em desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas críticas. Também preocupa-se com a estruturação de produção do conhecimento proveniente de fonte cibernética.

1.2 ESTRATÉGIA NACIONAL DE INTELIGÊNCIA

A Enint é um documento que fixa a Estratégia Nacional de Inteligência a ser adotada no Brasil, para a orientação estratégica decorrente da Política Nacional de Inteligência (PNI) e servindo de referência ao Plano Nacional de Inteligência. Além de consolidar conceitos, identifica os principais desafios para a Atividade de Inteligência de Estado, define eixos estruturantes e objetivos estratégicos, de modo a criar as melhores condições para que o país possa se antecipar às ameaças e usufruir das oportunidades existentes.

Seguindo a ideologia da END, a Enint também expressa sua preocupação com a segurança cibernética, pois faz parte do seu escopo estratégico. Assim, no desenvolvimento de seu ambiente estratégico, pode-se extrair da Enint (2017) a preocupação com a espionagem cibernética que cresce à medida que se eleva a utilização das ferramentas de TIC:

> Os inegáveis benefícios e facilidades trazidos pela utilização da tecnologia são, contudo, acompanhados de vulnerabilidades. Como consequência, o mundo enfrenta o crescimento da **espionagem cibernética**, inclusive com fins econômicos e científicos. Da mesma forma, outros riscos surgem com a evolução tecnológica: a automatização e a interconectividade dos sistemas de infraestruturas críticas, por exemplo, tornam possíveis sabotagens pela via cibernética. (grifos nossos).

A disseminação das ameaças cibernéticas provocou na intensificação das procuras por soluções que fossem capazes de aumentar o nível de segurança da informação, das comunicações e das infraestruturas críticas. De outro lado, há soluções de segurança, como os recursos criptográficos, que podem ser utilizados por grupos distintos dos interesses nacionais para a própria defesa.

É perceptível que a preocupação da Enint converge com a da END, elegendo os ataques cibernéticos como ameaças a serem observadas. Nesse ponto, é oportuno citar os conceitos de ameaça e de ataques cibernéticos dessa Estratégia. Consideram-se ameaças "aquelas que apresentam potencial capacidade de pôr em perigo a integridade da sociedade e do Estado e a segurança nacional" (BRASIL, 2017) e ataques cibernéticos

> ações deliberadas com o emprego de recursos de TIC para interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados essenciais à sociedade e ao Estado, a exemplo daqueles pertencentes à infraestrutura crítica nacional. (BRASIL, 2017).

As oportunidades que o Brasil está inserido proporcionam uma potencial capacidade de posicionar o país em um outro patamar competitivo e auxiliam na promoção e na defesa dos interesses do Estado e da sociedade brasileira. Uma delas, de acordo com a Enint, é a Inteligência cibernética, que evidencia a importância de se ter o domínio das soluções tecnológicas mais avançadas para lidar com o espaço cibernético, porque isso proporciona vantagens significativas às nações. Nesse

ambiente cibernético de ameaças e oportunidades, países que se desenvolvem mais rapidamente se tornam mais aptos a alcançar os objetivos nacionais.

Após as oportunidades serem definidas, desafios foram identificados, como por exemplo: a maior utilização de tecnologia de ponta, em especial no campo cibernético. Haja vista a necessidade de investimento para a atualização constante dos recursos tecnológicos indispensáveis à Atividade de Inteligência, que potencializam a eficácia do seu desempenho. Principalmente no espaço cibernético, a identificação de oportunidades e a previsão de fatos possivelmente danosos aos interesses nacionais são decisivos para elevar a efetividade do combate às ameaças virtuais.

A Enint definiu 33 objetivos estratégicos para o desempenho eficaz da Atividade de Inteligência, considerando um intervalo de 5 anos, tomando como base os desafios estratégicos identificados. Esses objetivos não seguem uma ordem de prioridade, mas retratam o foco estratégico para o direcionamento de esforços e a sinalização dos resultados essenciais a serem atingidos pelo Sistema de Inteligência Brasileiro. Dentre os objetivos, há dois que estão alinhados diretamente com este estudo: ampliar a capacidade do Estado na obtenção de dados por meio da Inteligência Cibernética; e promover a qualificação técnica para proteção e exploração do campo cibernético.

O primeiro objetivo estratégico tem como propósito ampliar a capacidade do Estado na obtenção de dados por meio da Inteligência Cibernética. Isso demonstra a preocupação em desenvolver a aptidão de fazer e compreender como obter dados no ambiente virtual, contornando o crescente aprimoramento das TIC. O segundo objetivo se propõe à promoção da qualificação técnica para o desenvolvimento e a exploração do campo cibernético. Os dois objetivos apresentados estão interligados, pois com a qualificação técnica há a possibilidade de ampliar a capacidade de obter, proteger e explorar dados e informações no campo cibernético.

Dessa forma, oportuno comentar que a Enint segue uma linha de raciocínio similar a da END, tanto a Atividade de Inteligência quanto a Defesa Nacional propõem a qualificação como uma orientação na obtenção de capacidade técnica na atuação de defesa contra ataques cibernéticos.

2 ATAQUES CIBERNÉTICOS

Os ataques cibernéticos têm ocorrido em todo o mundo, afetando diversas organizações do setor público e do privado, indistintamente, como Fundo Monetário Internacional (FMI), Lockheed Martin, Google, Sony, Playstation, Hyundai, Credicard, Hospital do Câncer de Barretos, bancos privados, instituições públicas, tribunais de justiça de diversos estados, Ministério Público estaduais, Instituto Nacional de Seguridade Social - INSS, Petrobrás, ministérios, bancos públicos etc (CORRÊA; BOCCHINI, 2017).

Os ataques atingiram sites do governo bloqueando o acesso a dados e sistemas, obrigando o pagamento de resgate dos dados por meio de moedas digitais, como a bitcoin. Também alvo de ataques, estabelecimentos comerciais tiveram seus sites e sistemas invadidos por hackers, como o caso de 28 de junho de 2017, em que alguns dos hospitais que tratam pacientes com câncer foram invadidos e tiveram seus computadores paralisados, atrapalhando o tratamento de quimioterapia em algumas regiões do Brasil. Os ataques em equipamentos paralisaram atendimentos de emergência, adulterando exames e induzindo médicos a erros e até impedindo que pacientes fossem medicados.

O Brasil é considerado o principal foco de crimes virtuais no mundo, sendo o 6º no ranking de ataques cibernéticos. Em 2017, o Brasil foi alvo de aproximadamente 205 milhões de ataques no ambiente virtual e estatísticas apontam que o país perdeu cerca de 22 bilhões com esses ataques. Sobre o assunto, Cortez e Kubota (2013) comentam que:

No Brasil, esse fato também vem ganhando importância após uma série de intrusões e ataques cibernéticos a bancos e a sistemas de órgãos do Governo Federal. Esses ataques revelaram ao grande público a existência de ameaças que têm o potencial de comprometer o pleno funcionamento de infraestruturas críticas.

Esses ataques são ameaças identificadas tanto pelo Estado quanto pela sociedade, os quais devem ser combatidos. Por isso, a Defesa Nacional e a Inteligência de Estado previram em suas estratégias essa preocupação. Ambos trabalham com o objetivo de capacitarem seu corpo técnico para a salvaguarda de dados e informações em âmbito nacional, evitando altos prejuízos decorrentes de ataques cibernéticos.

CONCLUSÕES

Este trabalho teve como objetivo analisar o olhar dos órgãos que se preocupam com Segurança Cibernética, como a Defesa Nacional e a Inteligência de Estado, tendo em vista as vulnerabilidades digitais existentes. Os ataques cibernéticos estão cada vez mais crescentes e provocam prejuízos de larga escala, comprometendo as economias afetadas. Por isso, a importância de se estudar esse assunto.

A normatização da Defesa Nacional e da Inteligência de Estado quanto à defesa cibernética demonstra a preocupação de ambas no combate ao cibercrime, por meio da obtenção, proteção e exploração de dados e informações no campo cibernético. Ficou evidente que ambas as instituições trabalham seguindo a mesma linha de raciocínio, tendo em vista que em suas estratégias objetivam promover uma maior capacitação do seu corpo técnico sobre assuntos relacionados à “defesa cibernética”, possibilitando elevar a capacidade de atuação nos momentos de crise. Essa evidência foi obtida por meio da análise das Estratégias Nacional de Defesa e de Inteligência.

Pelo fato desse assunto ser constantemente debatido e os ataques acontecerem corriqueiramente, o que justifica a elevada importância da temática, indicamos como sugestão a continuidade deste estudo, com novos olhares, evidenciando o impacto econômico desses ataques para a nação, os possíveis prejuízos financeiros e se esses ataques geram efeitos no produto interno bruto brasileiro.

CYBER SECURITY: THE VIEW OF NATIONAL DEFENSE AND STATE INTELLIGENCE IN THE DIGITAL VULNERABILITY

Abstract. This article is about cyber security, a current paradigm that is generating a growing concern of public and private entities around the world. In the past the threats were, for the most part, visible and tangible. But with the advancement of communication and information technologies, this has changed. The current threats are invading corporate electronics systems, hampering their activities. Faced with this, there are concerns for a new form of security and protection against digital vulnerabilities: cyber security. Cyber security is a current and growing concern of several institutions, both public and private. The concern is latent and is already standardized in the public policies of public security institutions, as is evident in the National Strategies of Defense and National Intelligence. This article demonstrates this standardization and consequent concern, both in the Defense area and in the area of Intelligence. Also, there are cyber attacks that occurred in some public and private institutions. Concern for a new form of defense is needed for institutions working safely. How to safeguard the sites and systems of your institutions? Is it possible to defend against these types of attacks, or are we at the mercy of cyber attacks?

Keywords: Cyber security. Digital vulnerabilities. National defense. National Defense Strategy. National Intelligence Strategy.

REFERÊNCIAS

BRASIL. Agência Brasileira de Inteligência. **Plano Nacional de Inteligência**. Disponível em: <http://www.abin.gov.br/acesso-a-informacao/legislacao-de-inteligencia/coletanea-de-legislacao/politica-nacional-de-inteligencia/>. Acesso em: 29 maio 2018.

BRASIL. **Decreto sem nº**, de 15 de dezembro de 2017. Aprova a Estratégia Nacional de Inteligência.

BRASIL. **Decreto nº 8793**, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília: 2012.

CANONGIA, Claudia; MANDARINO JÚNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, v. 14, nº 29, p. 21-46, jul-dez 2009, 2009.

CARVALHO, Antônio Ramalho de Souza; MASCARENHAS, Carlos Cezar de; OLIVEIRA, Edson Aparecida de Araújo Querido. Ferramentas de disseminação do conhecimento em uma instituição de c,t&i de defesa nacional. **Revista de Gestão da Tecnologia e Sistemas de Informação**, Vol. 3, nº 2, 2006, p. 77-92.

CORRÊA, Douglas; BOCCHINI, Bruno. **Ataque hacker global afeta órgãos de governo e da justiça no Brasil**, em 12/05/2017. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2017-05/ataque-hacker-global-afeta-orgaos-de-governo-e-entidades-no-brasil>. Acesso em: 29 maio 2018.

CORTEZ, Igor Siqueira; KUBOTA, Luis Claudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. **Revista de Administração**, v. 48, n. 4, p. 757-769, out./nov./dez. 2013.

MANDARINO JÚNIOR, Raphael. **Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro.** Monografia aprovada no Curso de Especialização em Gestão da Segurança da Informação e Comunicações. Brasília: Universidade de Brasília - UnB/ Departamento de Ciência da Computação, jun. 2009. p. 29.

O autor é mestrando em Economia da Defesa pela Universidade de Brasília – UnB, pós-graduado em Controladoria Governamental e em Gestão Pública pelo Instituto Federal de Brasília - IFB e graduado em Ciências Contábeis pela Universidade Federal de Sergipe - UFS. Possui cursos na área de Orçamento Público, Contabilidade, Administração, Inteligência e Fotografia. Atualmente, exerce a função de agente técnico em órgão do Gabinete de Segurança Institucional (GSI/PR). Já lecionou em cursos de nível técnico e superior as matérias de Contabilidade, Custos no Setor Público, Controladoria, Administração Financeira, Legislação Trabalhista, Gestão Bancária, Lei de Responsabilidade Fiscal e Ética Profissional. Pode ser contatado pelo e-mail prof.alexsandrobarreto@gmail.com.

CICAD.I.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

APLICABILIDADE DE REGRAS DE ENGAJAMENTO À GUERRA CIBERNÉTICA À LUZ DO DIREITO INTERNACIONAL DOS CONFLITOS ARMADOS

Ronald Felipe de Paula Santana
Pós-Graduado em Oficial de Comunicações

RESUMO: A Guerra Cibernética é um tema extremamente atual. Isso porque ainda que não caracterizado por uma guerra propriamente dita, observamos incidentes cibernéticos ocorrendo diariamente. No entanto, ainda não está muito claro quais legislações internacionais podem regular o meio ou o método de se fazer determinado ataque, levando em conta que o caminho usado para invadir um computador e roubar uma senha de banco é o mesmo usado para atacar uma rede de distribuição de energia e parar toda uma nação. A fim de determinar como preencher essa lacuna e verificar a viabilidade de se adotar regras de engajamento, foi realizada uma pesquisa aplicada, qualitativa e exploratória, baseada em uma pesquisa bibliográfica minuciosa com o intuito de subsidiar uma resposta à hipótese levantada. Fica claro o entendimento unânime acerca da aplicabilidade do Direito Internacional dos Conflitos Armados à Guerra Cibernética e completo alinhamento do Brasil e da doutrina de emprego do Exército Brasileiro com esse conjunto de normas. O país pode demonstrar seu comprometimento com a legislação internacional humanitária vigente reafirmando sua liderança regional. Isso poderá ser feito por meio da adoção de regras de engajamento.

Palavras-chave: Direito Internacional dos Conflitos Armados. Direito Internacional Humanitário. Guerra Cibernética. Regras de Engajamento.

INTRODUÇÃO

O Exército Brasileiro(EB) encontra-se em um processo de evolução, buscando o constante aperfeiçoamento de sua doutrina para uma Força Terrestre mais eficiente. Assim, pesquisas científicas na área de Operações Militares são importantes, considerando que trarão subsídios para alcançar o nível de prontidão e operacionalidade buscado.

O Direito Internacional dos Conflitos Armados (DICA) surgiu formalmente em 1864 com as Convenções de Genebra. Já o conceito de Guerra Cibernética é algo mais recente e no âmbito do Exército tem avançado exponencialmente desde 2008. Considerando que o Brasil é signatário das Convenções de Genebra e de seus protocolos adicionais, bem como outros tratados do DICA, é conveniente que se estude a possibilidade de se propor regras de engajamento para as ações de guerra cibernética.

Sendo assim, é viável que se aplique regras de engajamento à guerra cibernética considerando a legislação vigente no DICA e a doutrina de emprego do Exército Brasileiro para as operações de guerra cibernética? Será trabalhada a hipótese de que é viável que se aplique regras de engajamento que limitem os meios e métodos a serem empregados na guerra cibernética.

O objetivo geral desta pesquisa é verificar a viabilidade da aplicação de regras de engajamento à guerra cibernética no âmbito do EB, levando em consideração o Protocolo I adicional às Convenções de Genebra. Os objetivos específicos serão os seguintes: analisar a doutrina de guerra cibernética do Exército com a finalidade de determinar se é viável que se aplique regras de engajamento em consonância com o DICA; identificar a legislação humanitária internacional vigente que possa limitar as ações de guerra cibernética.

Também é importante que se apresente os principais conceitos que nortearam este trabalho. Sobre guerra cibernética, tem-se o seguinte:

> corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C2 ao adversário, explorá-las, corrompê-las, degradá-las ou destruí-las. (BRASIL, 2017).

Em se tratando de DICA, o conceito é o que segue:

> na atualidade, o DICA representa um conjunto de normas de proteção dos indivíduos e bens nos conflitos armados, além de disciplinar o comportamento dos Estados em tais conflitos, no tocante aos métodos e aos meios permitidos pelo Direito na condução das hostilidades. (BRASIL, 2011).

Este estudo é de fundamental importância, uma vez que adotar regras de engajamento poderia dar uma maior expressividade internacional ao Exército Brasileiro e ao Brasil, além de se vislumbrar um entendimento mundial acerca deste tema tão atual.

1 METODOLOGIA

Levando em consideração o problema apresentado, com o viés de atingir o objetivo que foi proposto, desde o mês de março de 2018, quando iniciada as pesquisas, foi feita uma abordagem qualitativa, estudando particularidades do tema abordado, buscando tendências, pensamentos ou opiniões acerca do tema, realizando observações.

A pesquisa foi de natureza aplicada, uma vez que não se buscou criar um conhecimento novo, mas sim, o estudo de pesquisas já existentes, que pudessem resultar em algo mais palpável, de fácil manipulação por parte de outros pesquisadores em uma oportunidade futura.

Desde seu início, essa pesquisa se caracterizou como exploratória quanto ao seu objetivo, uma vez que se iniciou com um minucioso levantamento bibliográfico com a finalidade de aperfeiçoar ideias já existentes sobre o assunto.

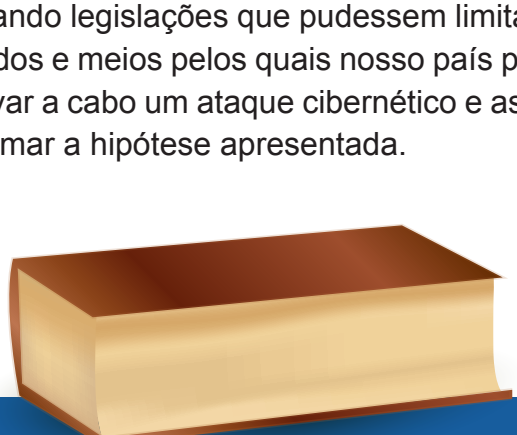
Isso conduziu este trabalho a uma pesquisa bibliográfica e após leitura analítica da literatura selecionada e fichamento das informações mais relevantes e pertinentes, chegar a conclusão desejada ao fim do mês de maio.

Foram feitas algumas visitas ao Comando de Defesa Cibernética, na segunda e terceira semanas de abril, com o intuito de coletar dados mais minuciosos. Diversos materiais foram disponibilizados, no entanto, alguns se revestem de um certo sigilo, considerando que, ainda, estão em fase de estudo doutrinário para posterior emprego pela Força Terrestre ou, até mesmo, pelas demais Forças Armadas. Isso limitou, de certa forma, a pesquisa, inviabilizando o emprego de outros instrumentos como entrevistas ou questionários.

Há uma vasta literatura que fala isoladamente sobre regra de engajamento ou guerra cibernética ou Direito Internacional dos Conflitos Armados. Entretanto, pouco foi encontrado ligando a guerra cibernética e o DICA e nada foi encontrado ligando essas três palavras-chave, que norteiam essa pesquisa.

Sendo assim, o artigo faz exatamente essa ligação, analisando o que motivou o Exército a voltar suas vistas para o setor cibernético, a doutrina de emprego decorrente disso e a interação com a legislação internacional humanitária.

Explorou-se a importância do DICA e do nosso país em respeitar essas normas, bem como qual a relação existente entre o DICA e a guerra cibernética que nos permitisse de alguma forma adotar regras de engajamento, considerando legislações que pudessem limitar os métodos e meios pelos quais nosso país poderia levar a cabo um ataque cibernético e assim, confirmar a hipótese apresentada.



2 RESULTADOS E DISCUSSÕES

2.1 O SETOR CIBERNÉTICO E O EXÉRCITO BRASILEIRO

O setor cibernético vem crescendo exponencialmente, sobretudo neste início de século. O governo brasileiro, atento às novas demandas tecnológicas, elaborou a Estratégia Nacional de Defesa(END). Este documento determina que os setores estratégicos espacial, nuclear e cibernético são essenciais para a defesa nacional e devem ser fortalecidos (BRASIL, 2008).

Em 2009, diretriz do Ministério da Defesa(MD) determinou que o setor cibernético ficaria sob coordenação do Exército e ainda destacou o fato de não haver qualquer tipo de tratado e controle internacional acerca deste setor (BRASIL, 2009).

Seguindo essa determinação, em 2010, foi criado o Centro de Defesa Cibernética(CDCiber), para fazer a coordenação e integração dos esforços da defesa cibernética. Posteriormente, foi criado o Comando de Defesa Cibernética (Com D Ciber), sendo um Comando Operacional Conjunto que dentre outras, possui a missão de planejar, orientar e controlar as atividades doutrinárias no âmbito do Sistema de Defesa Cibernética.

Reafirmando a importância do setor para o Exército, O Livro Branco de Defesa Nacional destacou que uma das capacidades consideradas prioritárias para consolidação da Força é a atuação no espaço cibernético com liberdade de ação (BRASIL, 2012).

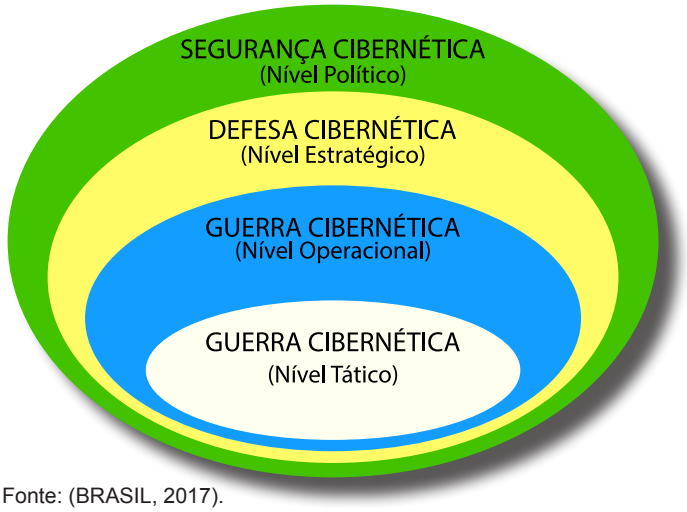
2.2 A GUERRA CIBERNÉTICA: PRINCIPAIS CONCEITOS E ASPECTOS DOUTRINÁRIOS

Já foi exposto sinteticamente o principal conceito de guerra cibernética, aquele encontrado no Manual EB70-MC-10.232: Guerra Cibernética, que hoje é utilizado pelo Exército. No entanto, Nunes (2015) dá uma maior amplitude a este conceito:

> São as ações ofensivas, defensivas e de exploração realizadas por meio de sistemas de informação e de redes de computadores, destinadas a interromper, negar, corromper, destruir ou acessar as informações contidas nos sistemas de TI inimigos e, ao mesmo tempo, garantir o uso continuado e a inviolabilidade dos nossos sistemas de TI. (NUNES, 2010 apud NUNES, 2015).

Segundo o MD, as ações no espaço cibernético não se encerram no EB, uma vez que se dividem de acordo com os níveis de decisão. A guerra cibernética se insere nos níveis operacionais e táticos, e é no nível tático que se insere a Força Terrestre, como vemos na figura abaixo:

FIGURA 1 Níveis de decisão



Fonte: (BRASIL, 2017).

No nível tático, o Sistema de Guerra Cibernética do Exército(SGCEx) precisa ter determinadas capacidades operativas que são a proteção cibernética, a exploração cibernética e o ataque cibernético, sendo este último, o que mais interessa ao escopo deste trabalho e tem a seguinte definição:

> Já o **Ataque Cibernético** é mais agressivo e, por intermédio dele, o atacante conseguirá derrubar ou corromper total ou parcialmente redes de dados e sistemas do oponente, danificar equipamentos e dispositivos ou destruir bancos de dados e informações relevantes, podendo para isso, fazer ou não uso de técnicas de invasão. (GOMES et al., 2016, grifo do autor).

No entanto, este ataque cibernético não deve ser feito de maneira aleatória, ne-

cessita estudo prévio que determine uma Lista de Alvos Cibernéticos (LIA Ciber) e uma Lista Priorizada de Alvos Cibernéticos (LIPA Ciber) (BRASIL, 2017).

Ainda sobre esses possíveis alvos, tem-se o que segue:

> A estrutura de guerra Cibernética da FTC pode, também, realizar tarefas ofensivas para negar serviço ou prejudicar o funcionamento das infraestruturas críticas do oponente localizadas no interior de sua zona de ação. (BRASIL, 2017).

Há um aspecto importante a ser destacado, daquilo que consta em Brasil (2017), que diz que "O ataque cibernético deve ser consistente com o arcabouço legal e normativo vigente".

2.3 O DICA E A LIMITAÇÃO DOS MEIOS E MÉTODOS

Nem sempre foi possível resolver situações controversas entre estados de maneira amistosa, através do diálogo, recorrendo-se muitas vezes à combates sangrentos, em guerras que por vezes se estenderam por longos anos. No entanto, uma constante se observa até os dias de hoje: o sofrimento que a guerra trás para as partes envolvidas.

Foi pensando nisso que em 1864 as Convenções de Genebra foram assinadas inicialmente por 16 países, inspirada nas propostas feitas por Henry Dunant em seu livro Memórias de Solferino, onde ele descreve as atrocidades da Batalha de Solferino e propõe normas que viriam a melhorar as condições das vítimas das Guerras.

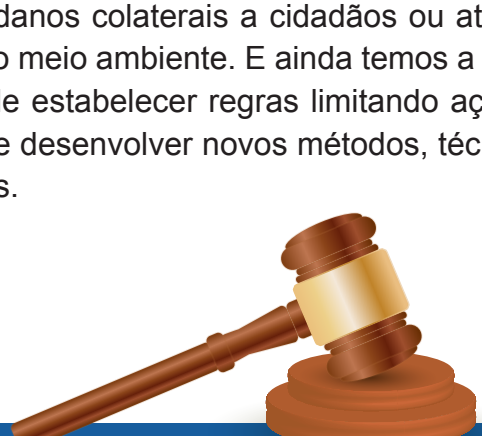
Com o passar dos anos, mais países inclusive o Brasil, aderiram às convenções e seus protocolos adicionais e demais tratados correlacionados:

> O Estado Brasileiro possui significativa predisposição em acatar as normas do Direito Internacional. O País ratificou ou aderiu a aproximadamente cinqüenta tratados multilaterais relacionados à proteção de pessoas e bens e à proibição de armas de destruição em massa. (BRASIL, 2011).

Assim, o Brasil promulgou por meio de decreto os protocolos adicionais às Convenções de Genebra, e especial destaque damos aos artigos 35 e 36 do protocolo I:

> **Artigo 35** – Regras fundamentais
>
> 1. Em qualquer conflito armado, o direito de as Partes em conflito escolherem os métodos ou os meios de guerra não é ilimitado.
>
> 2. É proibido utilizar armas, projéteis e materiais, assim como métodos de guerra de natureza a causar danos supérfluos ou sofrimento desnecessário.
>
> 3. É proibido utilizar métodos ou meios de guerra concebidos para causar, ou que se possa presumir que irão causar, danos extensos, duradouros e graves ao meio ambiente natural.
>
> **Artigo 36** — Armas novas
>
> Durante o estudo, preparação ou aquisição de uma nova arma, de novos meios ou de um novo método de guerra, uma Alta Parte contratante tem a obrigação de determinar se sua utilização seria proibida, em algumas ou em todas as circunstâncias pelas disposições do presente Protocolo ou por qualquer outra regra de direito internacional aplicável a essa Alta Parte contratante. (BRASIL, 1993).

Ainda que não exista no DICA ou Direito Internacional Humanitário(DIH) legislação específica que limite a maneira de conduzir a Guerra Cibernética por meio de um ataque a determinado Estado, se observarmos os artigos citados, vemos que não podemos atacar alvos de maneira irrestrita, sem preocupação com danos colaterais a cidadãos ou até mesmo ao meio ambiente. E ainda temos a obrigação de estabelecer regras limitando ações no ato de desenvolver novos métodos, técnicas e armas.



2.4 PRINCIPAIS CASOS DE ATAQUES CIBERNÉTICOS

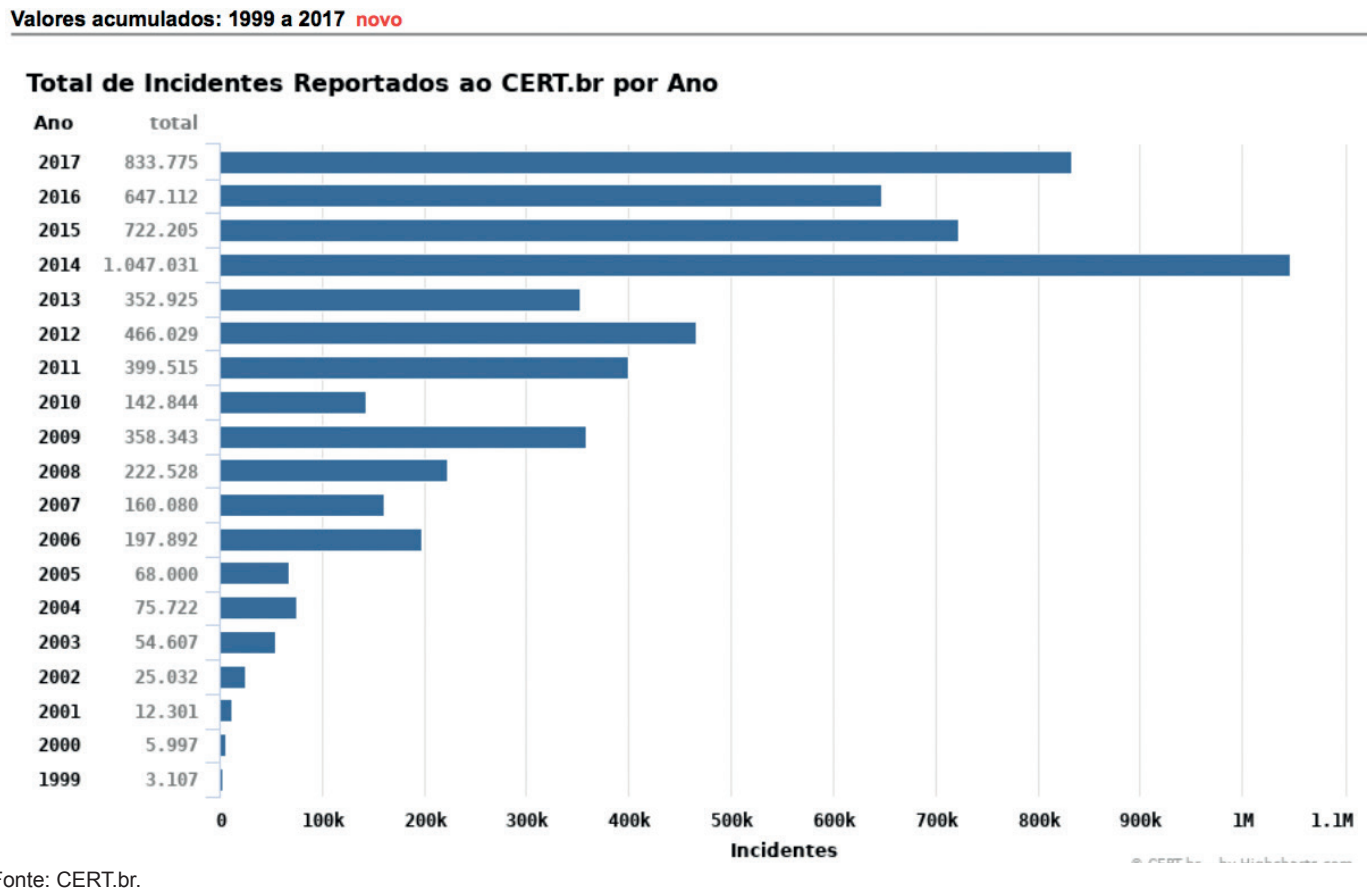
A atribuição de responsabilidade seja a Estados ou indivíduos fica dificultada pela ação de hackers que apesar de possuírem uma nacionalidade específica, não necessariamente atuam a mando de um País. Abaixo, no QUADRO 1, vemos uma síntese da evolução dos malwares, que caracterizam uma das formas de ataque por parte desses hackers:

QUADRO 1 Evolução histórica dos malware

1971	CREEPER - primeiro programa viral autorreplicante, foi escrito por Bob Thomas. Este vírus infectava computadores rodando o sistema operacional Telex e se espalhou via a ARPANET.Não causava dano, apenas apresentava uma mensagem na tela do computador infectado.
1981	ELK CLONER - vírus escrito para sistemas Apple II, causou a primeira infecção em larga escala.
1986	THE BRAIN - também conhecido como "Pakistani Flu", vírus que infectava o setor de "boot", foi o primeiro a infectar computadores tipo IBM-PC e causou uma epidemia global.
1988	MORRIS WORM - infectava sistemas rodando BSD Unix, foi o primeiro "worm" a se espalhar extensivamente.
1992	MICHELANGELO - causou grande preocupação devido à previsão de que infectaria milhões de computadores. Danos reais foram mínimos.
2003	SQL SLAMMER - também conhecido como "Saphire worm", trata-se de um worm que atacava vulnerabilidades do Microsoft SQL, foi o worm de mais rápida propagação, impactando a internet em apenas 15 minutos.
2010	STUXNET - primeiro worm a atacar sistemas SCADA (supervisory control and data acquisition).
2011	DUQU - worm relacionado ao stuxnet, porém sem possuir efetio destrutivo. Destinava-se a recolher informações.
2012	FLAME - na verdade foi um precursor do stuxnet que passou despercebido, usado em ciberespionagem contra o iran.

Fonte: (KUSHNER, 2013 apud NUNES, 2015).

GRÁFICO 1 Incidentes por ano no Brasil



Fonte: CERT.br.

Ataques acontecem diariamente no espaço cibernético, muitas vezes sendo de menor gravidade e geralmente não se caracterizam como de um Estado contra outro. No gráfico acima vemos o número crescente de ataques ou incidentes ocorridos no Brasil des-

de 1999, o que corrobora a posição de destaque do país como um dos mais atingidos por ataques.

Quando fazemos esta comparação entre ataques ou incidentes, Nunes (2015), diz o seguinte:

> Durante a primeira década do século atual, puderam ser observados vários incidentes cibernéticos que, se não chegaram a se configurar como ataques no contexto de uma guerra cibernética, ao menos tiveram grande repercussão e, pode-se dizer, constituíram os mais graves até então conhecidos (...).

É possível, ainda, observar na figura 2 um dos principais casos de ataques cibernéticos, através do malware Stuxnet, que "foi projetado para infectar sistemas industriais, no caso as centrífugas nucleares iranianas". (PONTE PINHEIRO, 2013).

Podemos ainda citar o ataque NotPetya, atribuído a Rússia e direcionado ao setor financeiro e energético da Ucrânia e que se estendeu por outros países da Europa, mostrando desrespeito com a soberania ucraniana.

Usinas nucleares, sistemas de controle de ferrovias, de tráfego aéreo, de fornecimento de energia são exemplos de infraestruturas críticas que se atacadas, podem causar sérios efeitos colaterais que vão além da vantagem militar, trazendo prejuízo para a população devido a seu impacto social, econômico e político. O Direito Internacional Humanitário é perfeitamente aplicável a este tipo de ação.

2.5 A APLICABILIDADE DO DIH PARA A GUERRA CIBERNÉTICA

Para Schimitt (2012), o espaço cibernético não é uma zona sem lei e os princípios da Lei Internacional são aplicáveis a esta área. Este mesmo autor foi o editor e o diretor da equipe que escreveu o Manual de Tallinn:

> O manual de Tallinn, que recebeu este nome em homenagem à capital da Estônia, local onde foi compilado, foi desenvolvido a pedido do Centro de Excelência em Defesa Cibernética Colaborativa da OTAN e aplica regras de comportamento de campos de batalha reais à internet. Seu objetivo é mostrar que uma guerra no mundo virtual pode se tornar real e, sendo assim, suas ações têm que ser submetidas às mesmas normas internacionais que regulam os combates nos campos de batalha. (GOMES et al., 2016).

O Comitê Internacional da Cruz Vermelha (CICV) acata com entusiasmo o que fala o Manual de Tallinn, além de nos remeter ao Protocolo I adicional às Convenções de Genebra:

> Avaliar a legalidade de novas armas é do interesse de todos os Estados, já que isso ajudará a assegurar que as suas forças armadas ajam em conformidade com suas obrigações internacionais. O artigo 36 do Protocolo I, de 1977, adicional às Convenções de Genebra exige que cada Estado-Parte se certifique que de que quaisquer novas armas que utilize ou considere utilizar cumpram com as regras de DIH, outro ponto proficuamente recordado pelo Manual de Tallinn. (INTERNATIONAL COMMITTEE OF THE RED CROSS, 2013, tradução nossa).

O Manual propõe 95 regras baseadas em leis internacionais consideradas aplicáveis no ato de disciplinar as ações de guerra cibernética. Ainda que tenha sido preparado a pedido da OTAN, não se trata de um tratado ou tampouco tem poder vinculativo, ou seja, nem mesmo os países membros da OTAN adotaram essas proposições como regras de engajamento ou atribuíram-na um valor legal, dando obrigatoriedade a seu cumprimento.

Ao falarmos de regras de engajamento, cabe ressaltar seu significado, uma vez que por meio dessas regras temos a possibilidade de limitar as ações de guerra cibernética:

> Caracteriza-se por série de instruções pré-definidas que orientam o emprego das unidades que se encontram na zona de operações, consentindo ou limitando determinados tipos de comportamento, em particular o uso da força, a fim de permitir atingir os objetivos políticos e militares estabelecidos pelas autoridades

> responsáveis. Dizem respeito a preparação e à forma de condução tática dos combates e engajamentos, descrevendo ações individuais e coletivas, incluindo as ações defensivas e de pronta resposta. (BRASIL, 2018).

Schimitt (2013) cita ainda no manual, qual o entendimento que os Estados Unidos têm acerca da aplicabilidade do DICA à guerra cibernética:

> O desenvolvimento de normas para a conduta do Estado no ciberespaço não requer uma reinvenção do direito internacional consuetudinário, nem torna obsoletas as normas internacionais existentes. As normas internacionais de longa data que orientam o comportamento do estado – em tempos de paz e conflito – também se aplicam no ciberespaço. (WHITE HOUSE CYBER STRATEGY, apud SCHIMITT, 2013, tradução nossa).

É pertinente ressaltar que dentro das estruturas criadas a partir da Estratégia Nacional de Defesa e diretrizes decorrentes, o Comando de Defesa Cibernética é a organização que tem a possibilidade de realizar estudos a fim de se estabelecer Regras de Engajamento para Guerra Cibernética. De acordo com pesquisas realizadas, têm sido feito análises doutrinárias neste sentido.

CONCLUSÕES

Ficou claro nesta pesquisa a importância que o governo brasileiro tem dado às questões que envolvem o setor cibernético, sobretudo a partir de 2008 com a criação da Estratégia Nacional de Defesa e desde então vemos uma sequência de ações e medidas que proporcionaram avanços significativos nesta área.

Uma vez atribuído ao Exército Brasileiro a coordenação das atividades neste setor, surgiram algumas organizações militares e iniciou-se o desenvolvimento de uma doutrina que viabilizasse o emprego da Força Terrestre não só para o ataque cibernético, mas também para defesa cibernética, considerando que o EB se insere no nível tático.

Por vezes, menos danosos à população de uma maneira geral, vimos que é grande a quantidade de incidentes cibernéticos que ocorrem no Brasil. É extremamente positivo que pensemos em como nos defender de tais situações que em dado momento, pode vir a se caracterizar como um verdadeiro ataque cibernético contra nossa soberania, como alguns que citamos neste trabalho.

E quando pensamos em ataques, não consideramos somente aqueles feitos contra nós, mas também o ataque a infraestruturas críticas da força oponente. Contudo, esse ataque não acontece de maneira irrestrita, havendo a necessidade de se estabelecer previamente uma lista de alvos a serem atacados.

Esta lista deve considerar o alcance dos danos causados por estes ataques. Ataques a sistemas de controle de tráfego aéreo, a usinas hidrelétricas, sistemas de controle de usinas de nuclear ou de redes de distribuição de energia, podem em um primeiro momento parecerem como um alvo militarmente compensador. Mas não podemos considerar apenas o valor militar desses alvos pois podem afetar serviços básicos utilizados por não combatentes, afetando o controle de voos comerciais, fornecimento de energia para hospitais e escolas, água potável, circulação de transporte público, entre outros. Esses danos colaterais não são aceitáveis e devem ser evitados ao máximo.

Resta sabido também que os ataques devem levar em consideração o arcabouço legal vigente, e isso nos remete ao Protocolo I adicional às Convenções de Genebra que de maneira tácita afirma que devemos limitar os meios e métodos utilizados em combate e devemos ao criar uma arma, técnica ou método, limitar a forma de emprego. O Comitê Internacional da Cruz Vermelha corrobora esse entendimento.

Cabe destacar também a grande contribuição do Manual de Tallinn que juntando a experiência de especialistas, propôs regras que garantem a aplicabilidade do DICA à Guer-

ra Cibernética.

Vale lembrar que pouco mais de 200 anos atrás, foi o livro de Henry Dunant que apresentou proposições que dariam origem ao primeiro conjunto de normas não consuetudinárias, que tinham poder vinculativo para as nações que assinaram as Convenções de Genebra. O mesmo pode acontecer com o Manual de Tallinn, podendo ser usado como um marco inicial ou até mesmo como uma referência, tanto pela Organização das Nações Unidas(ONU) quanto pelos países membros da OTAN.

Ora, se considerarmos que o Brasil acata essas normas do Direito Internacional, o Exército deveria considerar também essas normas no sentido de limitar os meios e métodos para a Guerra Cibernética.

As hipóteses de emprego (HE) de nossas Forças Armadas são diversas, no entanto, considerando os compromissos firmados internacionalmente pelo Brasil e que a própria doutrina determina que o ataque cibernético deve ser consistente com o arcabouço legal vigente, considero viável que se estabeleça regras de engajamento que tenham uma aplicação geral, em qualquer HE, limitando os meios e métodos utilizados para realizar um possível ataque num contexto de uma Guerra Cibernética. Isso permitiria que na fase de planejamento só se levantasse a possibilidade de atacar alvos que nos trariam estritamente a vantagem militar, auxiliando o decisor na tomada da melhor linha de ação e proporcionando uma melhor consciência situacional.

Tais regras ainda não são empregadas de maneira ostensiva por outros países que possuem notório saber no setor cibernético. Isso fica claro quando vemos ataques acontecendo com uma certa frequência e sua autoria sendo atribuída a países como a Rússia e os Estados Unidos.

Desde 2009 o próprio MD reconheceu que não há qualquer tratado internacional acerca deste setor. Sendo assim, o estabelecimento destas regras de engajamento por parte de nossas Forças Armadas traria um grande avanço para a área das operações militares, potencializando nosso reconhecimento internacional, o comprometimento entre as Forças e possivelmente nos alçando à vanguarda no que concerne à cibernética e ao respeito ao Direito Internacional Humanitário, reafirmando inclusive nossa liderança regional.

É extremamente importante que se prossiga nos estudos relacionados a este tema e até mesmo que outros pesquisadores brasileiros proponham regras de engajamento coerentes com nossa doutrina de emprego de guerra cibernética.

APPLICABILITY OF RULES OF ENGAGEMENT TO CYBER WARFARE UNDER THE INTERNATIONAL LAW OF ARMED CONFLICTS

Abstract. Cyber warfare is an extremely topical subject. This is because even though not characterized by a war itself, we observe cyber incidents occurring daily. However, it is still not very clear which international laws can regulate the means or method of making a particular attack, taking into account that the mean used to invade a computer and steal a bank password is the same used to attack a power distribution network and stop a whole nation. In order to determine how to fill this gap and verify the feasibility of adopting rules of engagement, an applied, qualitative and exploratory research was carried out, based on a thorough bibliographical survey with the intention of subsidizing a response to hypothesis raised. It is clear unanimous understanding of the applicability of the international law of armed conflicts to the cyber war and complete alignment of Brazil and the doctrine of employment of the Brazilian Army with this set of standards. The country can demonstrate its commitment to the existing humanitarian international legislation and its regional leadership. This can be done by adopting rules of engagement.

Keywords: Cyber Warfare. International Law of Armed Conflicts. International Humanitarian Law. Rules of Engagement.

REFERÊNCIAS

BRASIL. Ministério da Defesa. Exército Brasileiro. **EB70-MC-10.232: Guerra Cibernética**. 1. ed. Brasília: Estado Maior do Exército, 2017. Disponível em: <http://bdex.eb.mil.br/jspui/handle/1/631> Acesso em: 14 fevereiro

2018.

_____. Ministério da Defesa. **MD34-M-03: Manual de Emprego do Direito Internacional dos Conflitos Armados(DICA) nas Forças Armadas**. 1. ed. Brasília: Estado Maior Conjunto das Forças Armadas, 2011. Disponível em: < http://bdex.eb.mil.br/jspui/handle/123456789/140> Acesso em: 14 fevereiro 2018.

_____. DECRETO Nº 849, DE 25 DE JUNHO DE 1993. **Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados**. Brasília: Presidência da República (Casa Civil). Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0849.htm> Acesso em: 13 março 2018.

_____. Ministério da Defesa. Exército Brasileiro. **EB20-MF-03.109 Glossário de Termos e Expressões para uso no Exército**. 5. ed. Brasília: Estado Maior do Exército, 2018.

_____. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, 2008.

_____. Presidência da República. **Livro Branco de Defesa Nacional**. Brasília, 2012.

_____. Diretriz Ministerial nº 14. **Integração e Coordenação dos Setores Estratégicos da Defesa**. Brasília: Ministério da Defesa, 2012. Disponível em: <http://www.defesa.gov.br/arquivos/File/legislacao/emcfa/portarias/0014_2009.pdf> Acesso em: 24 abril 2018.

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTOS DE INCIDENTES DE SEGURANÇA NO BRASIL. **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponível em: <https://www.cert.br/stats/incidentes/> Acesso em: 02 maio 2018.

GOMES, Mauro Guedes Ferreira Mosqueira; CORDEIRO, Sandro Silva; PINHEIRO, Wallace Anacleto. **A Guerra Cibernética:** exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle (C2). Rio de Janeiro: RMCT Vol 33, n° 2, 2016. Disponível em: <http://rmct.ime.eb.br/arquivos/RMCT_3_tri_2016_web/RMCT_275.pdf> Acesso em: 17 abril 2018.

INTERNATIONAL COMMITTEE OF THE RED CROSS. **What limits the law of war impose on cyber attacks?** Genebra, 28 junho 2013. Disponível em: <https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm> Acesso em: 15 março 2018.

NUNES, Luiz Artur Rodrigues. **Guerra Cibernética e o Direito Internacional**: Aplicabilidade do Jus ad Bellum e o Jus in Bello. Rio de Janeiro: ESG, 2015. Disponível em: <http://www.esg.br/images/Monografias/2015/Nunes.pdf> Acesso em: 11 abril 2018.

PONTE PINHEIRO, Fábio. **A Cibernética como arma de Combate.** Rio de Janeiro: ESG, 2013. Disponível em: <http://200.143.206.219/images/Monografias/2013/PINHEIRO.pdf> Acesso em: 17 abril 2018.

SCHMITT, Michael. **Tallinn Manual on the International Law applicable to Cyber Warfare**. Cambridge. Reino Unido: Cambridge University Press, 2013.

_____. **International Law in Cyberspace:** The Koh Speech and Tallinn Manual Juxtaposed. Harvard, Estados Unidos: Harvard International Law Journal, 2012.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Possui especialização nas áreas de Operações de Paz e Operações Engenharia de Construção. Concluiu o curso Básico Paraquedista. Atualmente, exerce a função de Comandante de Companhia no 9° Batalhão de Engenharia de Construção e pode ser contatado pelo e-mail ronaldsantana88@hotmail.com.

CICAD.I.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

MEIO AMBIENTE

GERAÇÃO DE RECURSO NO REAPROVEITAMENTO DE BATERIAS DE RÁDIOS MILITARES: ESTUDO DE POSSIBILIDADE E VIABILIDADE

Matheus Braga do Nascimento
Pós-Graduado em Oficial de Comunicações

RESUMO: O descarte adequado de baterias inservíveis de rádios militares é uma das principais preocupações da Gestão Ambiental do Exército Brasileiro (EB), regulado por legislações internas e pela Política Nacional dos Resíduos Sólidos (PNRS). A PNRS enfatiza a importância da logística reversa como ferramenta que assegura a correta destinação dos resíduos sólidos, universo no qual se inserem as baterias. O presente estudo objetivou verificar como está sendo o descarte de baterias obsoletas no âmbito do EB, verificar se é legalmente possível gerar recurso no reaproveitamento dessas baterias, bem como a sua viabilidade. Por meio de pesquisa de campo foi possível levantar o processo de descarte de baterias no EB, identificar os tipos de baterias de dotação da Força Terreste, verificar a possibilidade de alguma forma de manutenção e reaproveitamento após o término da vida útil da bateria e por último levantar interesse de fornecedores e empresas na aquisição de baterias obsoletas. Ainda, foi levantado pela pesquisa bibliográfica e documental o amparo para o procedimento legal para alienação de bens inservíveis da União Federal, bem como sua utilização em prol da logística reversa. Por fim, foi possível analisar a viabilidade da geração de recurso em prol da logística reversa e da gestão ambiental.

Palavras-chave: Logística reversa. Leilão. Baterias. Gestão.

INTRODUÇÃO

O Exército Brasileiro (EB) faz uso constante de rádios como equipamento para estabelecer as comunicações quer seja em operações militares ao longo do território nacional, quer seja em situações rotineiras como, por exemplo, serviços de escala e coordenação de eventos (competições esportivas, formaturas, entre outros).

A grande maioria dos rádios militares utilizam baterias como fonte de energia e cada uma delas possui uma vida útil de acordo com o tipo e fabricante, e ao término da sua vida útil se torna inservível, sendo caracterizada como resíduo sólido e deve ter um descarte adequado, conforme prescreve a Lei nº 12.305/2010.

O descarte inadequado pode acarretar problemas ambientais, Kemerich et al. (2013) enfatizam o seguinte:

> Quando estes produtos não possuem mais utilidade, por carência de alternativas ou de informações, são despejados no lixo junto a resíduos sólidos comuns. Com o descarte indevido destes materiais, os metais pesados podem ser lixiviados infiltrando-se e contaminando o solo, o lençol freático, a fauna e a flora das regiões próximas e, também, pode prejudicar a saúde humana causando graves doenças que variam de lesões cerebrais a disfunções renais e pulmonares. (KEMERICH et al., 2013).

Para melhorar a coordenação e responsabilidades no correto descarte de resíduos sólidos, foi criado o conceito de logística reversa por meio Lei nº 12.305/2010 que prescreve o seguinte:

> instrumento de desenvolvimento econômico e social caracterizado por um conjunto de ações, procedimentos e meios destinados a viabilizar a coleta e a restituição dos resíduos sólidos ao setor empresarial, para aproveitamento, em seu ciclo

> ou em outros ciclos produtivos, ou outra destinação final ambientalmente adequada. (BRASIL, 2010).

O Exército Brasileiro se enquadra como consumidor dentro do contexto da logística reversa e deve adotar procedimentos corretos quanto ao descarte de resíduos sólidos, de forma a contribuir para a gestão ambiental, conforme prevê as Instruções Reguladoras para o Sistema de Gestão Ambiental no Âmbito do Exército (IR 50-20).

De acordo com a Política Nacional dos Resíduos Sólidos (PNRS), é possível que empresas e comerciantes dos resíduos sólidos em seu Art. 33 comprem produtos usados, como uma das formas de controlar e fiscalizar a correta destinação deles.

O estudo deste trabalho verificou a possibilidade e viabilidade de geração de recursos financeiros no reaproveitamento de baterias inservíveis dos rádios militares, em prol da logística reversa, levando em consideração as legislações ambientais e de alienação de bens inseríveis da união federal.

1 METODOLOGIA

O presente trabalho verificou como é, atualmente, o processo de descarte de material classe VII, universo em que se insere as baterias dos rádios militares, no Exército Brasileiro por meio de consulta às Normas Administrativas Relativas ao Material de Comunicações e Guerra Eletrônica (NARM Com GE) que prescreve os procedimentos logísticos relativos aos materiais classe VII do Exército Brasileiro

O Chefe da Seção de Manutenção do Comando de Comunicações e Guerra Eletrônica do Exército (Cmdo Com GE Ex) foi entrevistado com o objetivo de verificar como é, atualmente, o fluxo de descarte das baterias no Exército Brasileiro.

Foi verificado quais são os principais tipos de baterias utilizados pelos rádios militares, bem como a possibilidade de manutenção ou reaproveitamento por meio de entrevista a um técnico da Seção de Manutenção do Cmdo Com GE Ex.

Levantou-se o interesse de aquisição de baterias velhas por meio de questionário para duas empresas fabricantes e três empresas do ramo de reciclagem e reaproveitamento de resíduos sólidos.

Foram pesquisadas as legislações que amparam a alienação de bens inservíveis da União Federal e legislações ambientais vigentes no Brasil.

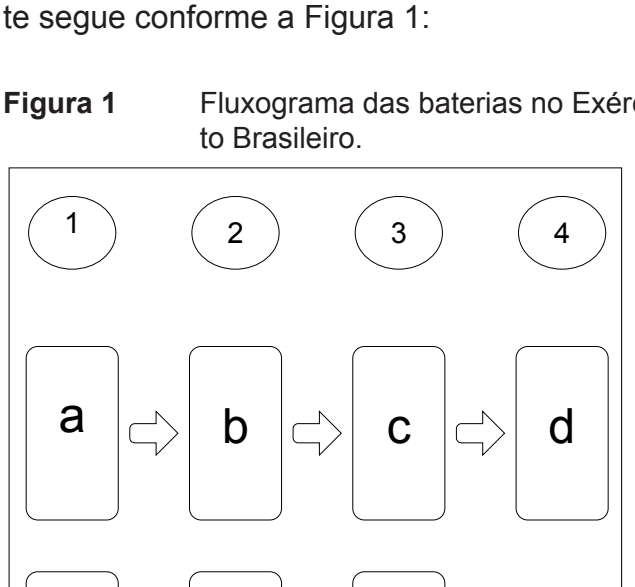
Procurou-se publicações de outros órgãos públicos que já efetuaram alienação de resíduos sólidos previstos pela Lei nº 12.305 por meio de leilão, com o objetivo de exemplificar a possibilidade de realizar tal procedimento para as baterias inservíveis.

2 RESULTADOS/DISCUSSÃO

O estudo identificou que as baterias são materiais de consumo, conforme o Anexo I da Portaria nº 448, de 13 de setembro de 2002, que divulga detalhamento das naturezas de despesa 339030, 339036, 339039 e 449052.

Verificou-se que o seu ciclo de descarte segue conforme a Figura 1:

Figura 1 Fluxograma das baterias no Exército Brasileiro.



Fonte: (ANDRADE; FONSECA; MATTOS, 2010).

LEGENDA:

1 - OM
2 - OM Manutenção
3 - Cmdo Com GE Ex
4 - fornecedor
a - enviar as baterias inservíveis para a OM de manutenção apoiadora
b - receber as baterias inservíveis das OM apoiadas e mediante acerto repassar ao Cmdo Com GE Ex.
c - receber as baterias inservíveis das OM de manutenção via cadeia de Comando e, após acúmulo significativo, remeter ao fabricante ou armazená-las até outra possível destinação.
d - fiscalizar o correto descarte das baterias de sua responsabilidade.
e - fornecer baterias novas para as OM de manutenção, se houver disponibilidade em estoque, analisando a necessidade e prioridade das OM.
f - receber as baterias novas do Cmdo Com GE Ex e gerenciar a distribuição, conforme necessidade das OM apoiadas
g - receber baterias novas da OM de manutenção apoiadora

Foi verificado que os principais tipos de baterias dos rádios militares são os seguintes: Lítion – Ion (LI-Ion), Niquel – Cádmio (Ni-Cd) e Níquel – Hidreto Metálico (Ni-Mh).

Pode-se verificar que não existe procedimento que possa realizar manutenção e recuperar as baterias após sua vida útil, e conforme consta na Figura 1, as baterias geralmente retornam aos fabricantes que por sua vez devem fiscalizar o correto descarte por meios próprios ou de empresas especializadas em reciclagem ou descarte de resíduos sólidos.

Verificou-se que é possível realizar geração de recursos na alienação de baterias inservíveis por meio de leilão, pois é o método legal para se vender os bens inservíveis da União Federal conforme prescreve o Art nº 17 da Lei 8.666, de 21 de junho de 1993.

Foi constatado que o Exército Brasileiro não tem realizado leilões de baterias especificamente, contudo há outros órgãos públicos que conseguem realizar leilão de produtos eletroeletrônicos e seus componentes, que inclusive se caracteriza como resíduo sólido amparado pela logística reversa, conforme prescreve o Art 33 da Lei 12.305, de 02 de agosto de 2010.

Verificou-se que outros órgãos realizam leilão de equipamentos eletrônicos obsoletos, que se enquadra no inciso VI do Art 33 da Lei 12.305, de 02 de agosto de 2010. Os equipamentos eletrônicos que não possuem mais vida útil, mais especificamente os monitores, microcomputadores e impressoras são armazenados até atingirem um volume considerável para a realização de leilão (DORRESTEIJN, 2015).

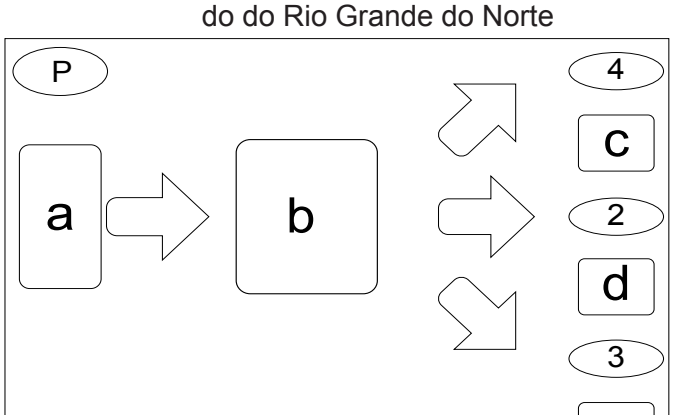
Pode-se observar na Tabela 1 um exemplo de materiais inservíveis sendo destinados para a execução do leilão pela Universidade de Brasília (UnB). Verificou-se que uma universidade pública do Rio Grande do Norte realiza a prática de leilão de resíduos eletrônicos de informática. De acordo com Andrade; Fonseca; Mattos (2010), a universidade denominada na pesquisa como Instituição 1, ao verificar que um equipamento eletrônico de informática chegou ao final de sua vida útil, realiza uma triagem com os materiais que se pretende leiloar em lotes, modificando sua condição de equipamentos para sucata, conforme pode-se observar na Figura 3.

TABELA 1 Resíduos Eletroeletrônicos leiloados pela UnB em 2014

Ordem	Descrição	Valor Inicial
1	Sucata de informática: (hub/concentrador), monitores, estabilizadores, nobreaks, impressoras, gabinetes, teclados e retroprojetores.	R$350,00
2	Sucata de informática: gabinete, monitores e impressoras	R$150,00
3	Sucatas: fotocopiadora, estabilizadores, nobreak, impressoras e cabos diversos.	R$180,00
4	Sucata de informática: gabinetes, monitores, impressoras, hub/concentrador, retroprojetor e aparelhos telefônicos.	R$250,00
5	Sucata de informática: monitores, retroprojetores, gabinetes, teclados, estabilizadores, caixas acústicas e impressoras	R$250,00
6	Sucatas de informática: monitores.	R$100,00

Fonte: (DORRESTEIJN, 2015).

Figura 2 Fluxograma de gestão de resíduos eletrônicos nas Instituições do estado do Rio Grande do Norte



Fonte: (ANDRADE; FONSECA; MATTOS, 2010).

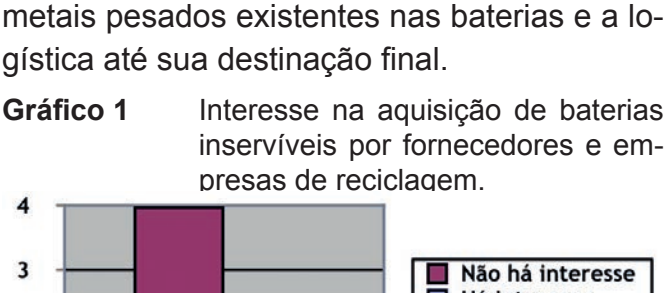
LEGENDA:

P - Parque de Informática Ativo
1 - Instituição 1
2 - Instituição 2
3 - Instituição 3
a - substituir os equipamentos velhos por novos, reaproveitando e realocando peças e equipamentos
b - triagem (descaracterização)
c - licitação modelo Leilão para sucateiros
d - acúmulo em depósito
e - doação para entidades de ensino e comunidades carentes.

Por meio do questionário aos fornecedores e empresas do ramo de reciclagem de resíduos sólidos, foi constatado que há pouco interesse por parte do setor comercial e empresarial na aquisição de baterias obsoletas e geralmente quando é feito se dá pela aquisição da bateria inserida num lote de outros resíduos eletroeletrônicos e seus componentes. De um universo de cinco empresas, apenas uma demonstrou interesse em adquirir baterias inservíveis, conforme consta no Gráfico 1.

O principal motivo pelo desinteresse de fornecedores e empresas se dá pelo fato do elevado custo gerado com a reciclagem dos metais pesados existentes nas baterias e a logística até sua destinação final.

Gráfico 1 Interesse na aquisição de baterias inservíveis por fornecedores e empresas de reciclagem.



Fonte: o autor, 2018.

CONCLUSÕES

Por meio da análise das legislações referentes à alienação de bens da União Federal, conclui-se que a geração de recursos no reaproveitamento de baterias inservíveis dos rádios militares é possível mediante realização de leilão.

A Política Nacional dos Resíduos Sólidos (PNRS) permite que fornecedores e comerciantes de resíduos sólidos, dentre os quais incluem-se baterias de equipamentos de rádios militares, comercialize-os, com o objetivo de serem recicladas ou aproveitadas de outra maneira. Criando-se, assim, uma alternativa adicional à logística reversa.

Verificou-se que há instituições públicas que leiloam resíduos eletroeletrônicos obsoletos em prol da logística reversa. Conclui-se que, de forma semelhante, é possível realizar tal procedimento com as baterias obsoletas dos rádios militares.

O estudo verificou que não há indícios de interesse na aquisição de baterias inservíveis de rádios militares. Por parte de fornecedores e das empresas do universo investigado.

Em virtude do exposto, infere-se que apesar de ser possível a geração de recurso no reaproveitamento de baterias de rádios militares, tende a ser inviável pela ausência de interessados em adquirir baterias inservíveis.

Outro empecilho para a realização de leilão é o fato de que não há como assegurar que, caso haja compradores, seja reaproveitado ou descartado adequadamente as baterias, criando-se, assim, a possibilidade de danos ambientais.

A linha de ação de leiloar baterias apresenta-se como uma solução interessante para a Administração Pública, do ponto de vista financeiro. Portanto, executar a logística reversa pode assegurar o benefício da preservação ambiental. Dessa forma, conclui-se que o Exército Brasileiro age conforme a legislação em vigor, sendo adequado manter tal procedi-

mento.

GENERATION OF RESOURCE IN THE REAPROVEMENT OF MILITARY RADIO BATTERIES: STUDY OF POSSIBILITY AND FEASIBILITY

ABSTRACT. PROPER DISPOSAL OF UNUSABLE BATTERIES OF MILITARY RADIOS IS ONE OF THE MAIN CONCERNS OF THE BRAZILIAN ARMY (EB) ENVIRONMENTAL MANAGEMENT, REGULATED BY DOMESTIC LEGISLATION AND THE NATIONAL SOLID WASTE POLICY (PNRS). THE PNRS EMPHASIZES THE IMPORTANCE OF REVERSE LOGISTICS AS A TOOL THAT ASSURES THE CORRECT DESTINATION OF SOLID WASTE, A UNIVERSE IN WHICH THE BATTERIES ARE INSERTED. THE PRESENT STUDY AIMED TO VERIFY HOW THE DISPOSAL OF OBSOLETE BATTERIES IS BEING CARRIED OUT WITHIN THE SCOPE OF THE EB, TO VERIFY IF IT IS LEGALLY POSSIBLE TO GENERATE A RESOURCE IN THE REUSE OF THESE BATTERIES, AS WELL AS THEIR VIABILITY. THROUGH FIELD RESEARCH IT WAS POSSIBLE TO RAISE THE PROCESS OF DISCARDING BATTERIES IN THE EB, IDENTIFY THE TYPES OF BATTERIES OF THE TERRESTRIAL POWER, CHECK THE POSSIBILITY OF SOME MAINTENANCE AND REUSE AFTER THE END OF THE BATTERY LIFE AND LASTLY RAISE THE INTEREST OF SUPPLIERS AND COMPANIES IN THE ACQUISITION OF OBSOLETE BATTERIES. ALSO, THE BIBLIOGRAPHIC AND DOCUMENTARY RESEARCH SUPPORTED THE LEGAL PROCEDURE FOR ALIENATION OF FEDERAL UNION'S WASTE GOODS, AS WELL AS ITS USE IN FAVOR OF REVERSE LOGISTICS. FINALLY, IT WAS POSSIBLE TO ANALYZE THE VIABILITY OF RESOURCE GENERATION FOR REVERSE LOGISTICS AND ENVIRONMENTAL MANAGEMENT.

KEYWORDS: REVERSE LOGISTICS. AUCTION. BATTERIES. MANAGEMENT.

REFERÊNCIAS

ACADEMIA MILITAR DAS AGULHAS NEGRAS. **Manual de metodologia da pesquisa científica**. Resende, 2008.

ANDRADE, R.; FONSECA, C.; MATTOS, K.**Geração e destino dos resíduos eletrônicos de informática nas faculdades e universidades de Natal**. São Carlos, SP, 2010. Disponível em: < web-resol.org/textos/enegep2010_tn_stp_121_788_15055.pdf >. Acesso em 29 Abr. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023**: informação e documentação: referências: elaboração. Rio de Janeiro. 2002.

_____.**NBR 6024**: numeração progressiva das seções de um documento: procedimento. Rio de Janeiro, 1989.

_____.**NBR 14724**: informação e documentação: trabalhos acadêmicos: apresentação. Rio de Janeiro, 2005.

BRASIL. **Decreto nº 99.658**, de 30 de outubro de 1990.

_____. **Lei nº 12.305**, de 02 de agosto de 2010.

_____. **Lei nº 8.666**, de 21 de junho de 1993.

_____. **Portaria nº 448**, de 13 de setembro de 2002. Divulga o detalhamento das naturezas de despesas 339030, 339036, 339039 e 449052. Disponível em <http://portalfns.saude.gov.br/images/banners/Sigem/Portaria_448_de_13_de_Setembro_de_2002.pdf>. Acesso em: 27 Abr. 2018.

_____. **Resolução CONAMA**, nº 401, de 04 de novembro de 2008.

_____. EXÉRCITO BRASILEIRO. **Portaria nº 232**, de 6 de abril de 2010.Aprova as Instruções Gerais para a Gestão de Material Inservível do Comando do Exército (IG 10-67) e dá outras providências. Disponível em: < www.11icfex.eb.mil.br/images/orientar_e_controlar/patrimonio/Port-232.pdf >. Acesso em: 27 Fev. 2018.

_____._____. **Portaria nº 001-DEC**, de 26 de setembro de 2011. Aprova as Instruções Reguladoras para o Sistema de Gestão Ambiental no Âmbito do Exército (IR 50 - 20). Disponível em < www.dpima.eb.mil.br/images/manuais/IR50-20.pdf>. Acesso em: 15 Abr. 2018.

COMANDO DE COMUNICAÇÕES E GUERRA ELETRÔNICA DO EXÉRCITO. **NORMAS ADMINISTRATIVAS RELATIVAS AO MATERIAL DE COMUNICAÇÕES E GUERRA ELETRÔNICA** – NARM Com. Brasília, 2017. Disponível em < http://www.ccomgex.eb.mil.br/index.php/2015-04-10-13-35-55>. Acesso em 20 Abr. 2018.

DORRESTEIJN, Amanda Melo. **Avaliação qualitativa e quantitativa da logística reversa do lixo eletrônico da Universidade de Brasília como subsídio para políticas de gestão no âmbito universitário**. 2015. Monografia (Bacharel em Ciências Ambientais) - Universidade de Brasília.

ESCOLA DE COMUNICAÇÕES. **INSTRUÇÕES DE PÓS-GRADUAÇÃO DA ESCOLA DE COMUNICAÇÕES IPG/EsCom** - EB60-CI-43.003. Brasília, 2017.

KEMERICH, P. D. C. et al. **Impactos Ambientais decorrentes da disposição inadequada de lixo eletrônico no solo**. 2013. Disponível em: <ferramentas.

unipinhal.edu.br/engenhariaambiental/include/getdoc.php?id=2556&article=900&mode=pdf>. Acesso em 21 Mar. 2018.

MOURA, L. M. R.; PEREIRA, S. V.; GUIMARÃES, H. B. **A Logística Revesera no Exército Brasileiro como instrumento de proteção ambiental**. 2017. Disponível em <www.eumed.net/rev/delos/30/logistica-reversa-brasil.zip> Acesso em 30 Abr. 2018.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Atualmente, exerce a função de oficial subalterno na Companhia de Engenharia de Equipamentos e Manutenção do 6° Batalhão de Engenharia de Construção e pode ser contactado pelo email matheusbn@gmail.com.

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

EDUCAÇÃO

DESAFIO DAS INSTITUIÇÕES DE ENSINO DO EXÉRCITO BRASILEIRO NA MODALIDADE DE ENSINO A DISTÂNCIA

José Erlan Nunes Matias
Graduado em Matemática

RESUMO: Este artigo tem por finalidade trazer as dificuldades enfrentadas pela instituição Exército Brasileiro na modalidade de ensino a distância. Em uma concepção mais específica, mostrar que o papel do novo instrutor traz novas responsabilidades e estas necessitam de novas técnicas no que tangem à organização didático-pedagógica. A educação a distância (EAD) traz algumas singularidades que não se enxerga na modalidade presencial, onde necessitam ser elencadas e trabalhadas em qualquer instituição que pretende utilizar essa modalidade no processo ensino-aprendizagem.

Palavras-Chave: Aprendizagem. Educação a Distância. Professor. Instrutor.

INTRODUÇÃO

Apesar de professores e alunos fazerem parte de um ambiente virtual na modalidade a distância, de cursos oferecidos por diversas instituições, inclui-se aqui as organizações públicas, não se pode afirmar que existe cooperação entre os envolvidos no processo ensino-aprendizagem. Face a essa problemática serão realizadas discussões quanto às ferramentas e conceitos pedagógicos utilizados para a aprendizagem cooperativa em um ambiente educacional virtual.

> Uma comunidade virtual é construída sobre as afinidades de interesses, de conhecimentos, sobre projetos mútuos, em um processo de cooperação ou de troca, tudo isso independentemente das proximidades geográficas e das filiações institucionais. (LÉVY, 2000, p. 127 apud SCHERER, 2014, p. 55).

Aliado ao viés corporativo no desenvolvimento de pessoas é mister abordar o caminho e ferramentas pedagógicas utilizadas nos ambientes virtuais no que tange ao design didático. O design didático tem como objetivo trazer conceitos e técnicas eficientes no planejamento e elaboração de cursos que tenham a Educação a distância (EaD) como modalidade, pois esses instrumentos serão de grande valia para a eficácia na aprendizagem.

Sabe-se que qualquer instituição tem como premissa qualificar seus recursos humanos, independente se é pública ou privada. Seus objetivos têm como horizontes o excelente desempenho do quadro de pessoal, novos conhecimentos e habilidades, e por consequência o desenvolvimento institucional. Para que isso ocorra de forma sistemática e profícua é interessante diferenciar informação de formação, esta que vem do latim *formatio* – dar forma a algo, constituir, formar, assim, modelar algo que desperte a curiosidade. Aquela vem do latim *informatio* - conceber ideia, dar forma - ou seja, um dado que pode agregar ou não no processo epistemológico.

> Desenvolver pessoas não se trata de um repasse de informações que visam ao aprendizado de novos conhecimentos, habilidades ou destrezas com o objetivo de que elas se tornem mais eficientes. O processo de formação é mais amplo e leva o indivíduo ao aprendizado de novas atitudes e adoção de uma postura pró-ativa, buscando idéias (sic) e soluções para os problemas vivenciados no trabalho. (VILAS BOAS e FILHO, 2007, p. 2).

Nesse contexto, e aproveitando o momento atual onde o Exército Brasileiro inicia seus passos no Ensino por Competência, é de suma importância analisar através de confrontos das ideias encontradas na bibliografia pesquisada o caminho a ser percorrido pelas ins-

tituições que têm a incumbência de ministrar conteúdos a distância em ambientes virtuais.

2 A EAD NAS INSTITUIÇÕES

Logo após a aprovação da Lei de diretrizes e Bases – LDB em 1996 cresceu significativamente o número de instituições públicas e privadas que ofertam cursos na modalidade a distância. Segundo os dados obtidos pela Associação Brasileira de Educação a Distância – ABED, entre 2014 e setembro de 2017 houve um aumento de 22% no número de instituições formadoras, indicando uma projeção significativa neste tipo de formação. Em 2017, vale destacar, 22% das instituições formadoras eram instituições educacionais públicas federais e órgãos públicos ou do governo. Esses dados apenas reforçam a necessidade de avanços nas questões estruturais e pedagógicas referentes à educação a distância, ou seja, a Tecnologia da informação (TI) deve dar lugar à Tecnologia da Informação e Comunicação (TIC) que traz um conceito mais dinâmico e pedagógico nos serviços e implementações.

2.1 A EAD NO EXÉRCITO BRASILEIRO

O Exército Brasileiro está adotando o Ensino por Competências como base metodológica para todos os cursos oferecidos pela instituição, trazendo a EaD como recurso educacional, deixando de lado o Ensino por Objetivos que tinha como barreira a compartimentalização dos saberes. As instituições de ensino estão adequando os currículos e avaliações de seus cursos por determinação da Portaria nº 125 – DECEx, de 23 de setembro de 2014, complementada pela Portaria nº 074 – DECEx, de 07 de março de 2017, que aprova as Instruções Reguladoras do Ensino por Competências no Exército Brasileiro. Por consequência, aconteceram mudanças significativas nos currículos e avaliações dos cursos ofertados pela instituição, fator que incentivou este trabalho. Importante destacar que não é objeto de estudo deste artigo o Ensino por Competências, porém esta modalidade trouxe como ferramenta intrínseca a educação a distância.

Essa inovação necessita de uma certa atenção, visto que muitas ferramentas pedagógicas deverão romper a barreira do tecnicismo.

> No âmbito do Exército, tal proposta representa um grande desafio, uma vez que as práticas de ensino estão fortemente alicerçadas no tradicionalismo e no tecnicismo. Sendo assim, a superação de um modelo fundamentado no ensino por objetivos que privilegia a fragmentação e a sequenciação de conteúdos em dinâmicas de aprendizagem com baixo grau de dialogicidade e complexidade constitui-se numa verdadeira batalha metodológica. Como se pode notar, não se trata apenas de modernizar ou aperfeiçoar técnicas de ensino, mas de desenvolver uma nova mentalidade pedagógica capaz de inspirar uma nova cultura de aprendizagem compatível com os desafios do século XXI. (DURAN, 2016, p. 5).

É importante destacar que o objeto de estudo são os cursos realizados no Exército Brasileiro destinados aos militares, assim, o universo considerado possui apenas adultos, circunstância que deve ser levada em consideração na modalidade de ensino a distância. Sabe-se que boa parte dos cursos e estágios são ministrados por militares da Força e que muitos não possuem a formação pedagógica que venha superar a barreira do tecnicismo, visto que muitas referências pedagógicas são da modalidade presencial, esta que fez parte da formação militar da maioria dos instrutores. Essa formação é orientada pelo Manual Técnico T21 - 250 – Manual do Instrutor aprovado pela portaria nº 092 – EME, de 26 de setembro de 1997, onde não traz o papel do novo instrutor, com novas funções. Essa preocupação é importante por diversos motivos, uma delas é que esse sujeito do processo ensino-aprendizagem terá algumas funções nos cursos semipresenciais ou totalmente a distância, podemos destacar a função de tutor que traz algumas peculiaridades pedagógicas na modalidade EaD, essas dificuldades serão discutidas mais adiante. As adversidades não estão apenas na instituição Exército, estão presentes na realidade educacional brasileira,

porém está melhorando gradativamente quanto às técnicas utilizadas na EaD, em virtude do aumento exponencial dos alunos matriculados nos cursos a distância e do avanço das tecnologias digitais de informação e comunicação. De acordo com Mugnol (2009),

> são também carentes de regulamentação o sistema de acompanhamento do aprendizado dos alunos, a formação dos professores, as diferentes metodologias utilizadas, a avaliação do resultado do processo de ensino aprendizagem (...).

Projetado por Freepik

3 OS DESAFIOS NA EAD

As TIC trazem uma falsa percepção quanto à evolução da educação a distância, bem como às técnicas pedagógicas utilizadas no ambiente virtual, dependendo da abordagem dessas técnicas estaremos apenas repetindo o processo ensino-aprendizagem no ensino por objetivos, como reitera Lapa e Beloni (2012, p.178) "(...) fazer da EaD uma educação "bancária" em maior escala."

Conforme Duran (2016), não é verdade que modelos pedagógicos estão progredindo em consequência do desenvolvimento tecnológico.

Muitos dos instrutores que fazem parte do corpo docente dos estabelecimentos de ensino do Exército Brasileiro são militares e aprenderam técnicas de cursos presenciais. As referências pedagógicas estão defasadas, o mais importante deveria ser a preocupação com a formação técnico-pedagógica do corpo docente que será referência futuramente àqueles que vislumbram fazer parte da área de ensino na instituição.

> Educação a distância é a aprendizagem planejada que geralmente ocorre num local diferente do ensino e, por causa disso, requer técnicas especiais de desenho de curso, técnicas especiais de instrução, métodos especiais de comunicação através da eletrônica e outras tecnologias, bem como arranjos essenciais organizacionais e administrativos. (MOORE e KEARSLEY, 1996, p.11, apud KELLER et al., 2009, p. 3).

Uma das dificuldades enfrentadas pelos instrutores é a função de tutor na EaD que faz parte de muitos cursos oferecidos pela instituição. A função de tutor requer um conhecimento que vai além do espaço virtual, não é apenas o conhecimento de técnicas eletrônicas que favorecê-lo. Como exemplo e classificando os sujeitos - professores e alunos - do processo ensino-aprendizagem na modalidade EaD conforme Scherer (2014) em: habitantes, visitantes e transeuntes, pode-se verificar com experiências vividas nestes espaços a situação de alunos que não participam dos diálogos e atividades que não "valem nota". É nítido o envolvimento obrigatório destas atividades, onde as mesmas não trazem desafios saudáveis e instigantes para estes alunos. Para Scherer e Brito (2014) os habitantes destes espaços "moram" nestes locais, organizam, participam, cooperam, ou seja, são corresponsáveis pelo ambiente educacional. Tem-se ainda os visitantes, sujeitos que não se sentem responsáveis pelo espaço, estão ali por outro motivo, não se responsabilizam, não moram naquele lugar. Por fim, os transeuntes, que estão apenas transitando, não habitam nem visitam. Estes, conforme Scherer e Brito (2014, p. 56),

> são parecidos com os 'zapeadores', aqueles que praticam o zapping com a televisão, internet, trocando de espaços, sem uma intenção em específico, sem saber para onde ir.

Observe que os habitantes, visitantes e transeuntes são alunos e professores, su-

jeitos do processo, porém quem deve planejar e coordenar as atividades inicialmente é o professor, roteirista desta modalidade educacional. Suas técnicas são responsáveis pelas atividades, elas devem trazer dinamicidade às ações praticadas neste habitat, são elas que estimulam a participação dos instruendos. Essa interação deve ser mediatizada com sujeitos concatenados, onde os mesmos devem fazer parte de um espaço desafiador e criativo.

Nesse sentido, o planejamento didático-pedagógico

> deve ser desafiador, desequilibrando cognitivamente o aluno ao ser questionado, deixando-o perplexo, em dúvida quanto às certezas que possui, ou à ação que pratica. A pergunta desafiadora oportuniza o pensar, o operar, (...); ela favorece a aprendizagem do aluno. (SCHERER e BRITO, 2014, p.58)

CONCLUSÃO

De maneira similar aos avanços da tecnologia da informação e comunicação, a educação de ensino a distância deve trazer inovações e romper o obstáculo chamado tecnicismo. Frente ao momento que a instituição Exército Brasileiro traz como novidade o Ensino por Competências, vale a preocupação em formar instrutores aptos a utilizarem todas as ferramentas pedagógicas a seu favor. As TICs devem ser apenas instrumentos que venham auxiliar seu quadro docente, que sabendo integrá-los ao conhecimento técnico-didático-pedagógico poderá renovar os espaços virtuais e desenvolver novas ferramentas referentes à comunicação e interação. O produto dessas inovações será um ambiente virtual desafiador e agregador, e para isso acontecer, deverá figurar como premissa pedagógica, a cooperação entre os sujeitos do processo ensino-aprendizagem.

A formação do corpo docente deverá ser um dos objetivos fundamentais neste processo de transformação, bem como a atualização do Manual do Instrutor, fator preponderante nessa renovação. Esse manual deverá nortear os instrutores não só na modalidade presencial, mas também na modalidade EaD, servindo de base comum às orientações e planejamentos na dimensão didático-pedagógica.

CHALLENGE OF BRAZILIAN ARMY EDUCATION INSTITUTIONS IN THE DISTANCE EDUCATION MODE

ABSTRACT. THIS ARTICLE AIMS TO BRING THE DIFFICULTIES FACED BY THE BRAZILIAN ARMY INSTITUTION IN THE DISTANCE LEARNING MODALITY. IN A MORE SPECIFIC CONCEPTION, TO SHOW THAT THE ROLE OF THE NEW INSTRUCTOR BRINGS NEW RESPONSIBILITIES AND THESE NEED NEW TECHNIQUES IN WHAT CONCERNS THE DIDACTIC-PEDAGOGICAL ORGANIZATION. THE DISTANCE EDUCATION BRINGS SOME SINGULARITIES THAT CAN NOT BE SEEN IN THE FACE-TO-FACE MODALITY, WHERE THEY NEED TO BE LISTED AND WORKED IN ANY INSTITUTION THAT INTENDS TO USE THIS MODALITY IN THE TEACHING-LEARNING PROCESS.

KEYWORDS: LEARNING. DISTANCE EDUCATION. TEACHER. INSTRUCTOR.

REFERÊNCIAS

BRASIL. Portaria nº 202 - DECEx, de 23 de novembro de 2016. Aprova as Normas para a Avaliação da Aprendizagem – 3ª Edição (NAA – EB60-N-06.004) e dá outras providências.

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

_____. Portaria nº 143 - DECEx, de 25 de novembro de 2014. Aprova as Normas para Desenvolvimento e Avaliação dos Conteúdos Atitudinais (NDACAEB60-N-05.013).

_____. Portaria nº 092 - EME, de 26 de setembro de 1997. Aprova o Manual Técnico T 21-250 - Manual do Instrutor, 3ª Edição, 1997.

DURAN, Débora. Educação a distância no Exército Brasileiro: o desafio da qualidade na educação militar. In: 22 CONGRESSO ABED DE EDUCAÇÃO A DISTÂNCIA, 2016, Águas de Lindóia. Anais do 22 Congresso ABED de Educação a Distância. São Paulo: ABED, 2016.

KELLER, J. ; SANTOS, N. ; Busanello, R. B. ; ESTÁCIO, S. N. . EaD e Aprendizagem Organizacional: Uma Análise de Relação e Possibilidades. RENOTE. Revista Novas Tecnologias na Educação, v. 7, p. 1-10, 2009.

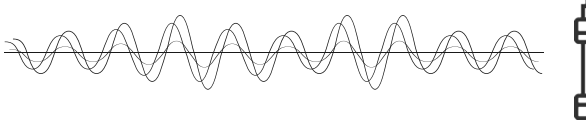
LAPA, A. B.; BELLONI, M. L. Educação a distância como mídia-educação. Perspectiva (UFSC), v. 30, p. 175-196, 2012.

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

VILAS BOAS, A. A.; CARVALHO FILHO, A. Educação a Distância em uma Organização Militar: parcerias e evasão. In: 13th Congresso Internacional de Educação a Distância, 2007, Curitiba. Anais do 13th Congresso Internacional de Educação a Distância. Sao Paulo: Associação Brasileira de Educação a Distância, 2007. p. 1-12.

O autor é Graduado em Licenciatura em Matemática pelo Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul. Exerce a função de monitor na Escola de Comunicações do Exército Brasileiro e pode ser contactado pelo e-mail erlanpe@gmail.com.

LICENÇA DE USO LIVRE

ARTE	AUTOR
	Projetado por rawpixel.com / Freepik
	Projetado por Creative_hat / Freepik
	Projetado por Freepik
	Projetado por Dondoni
	Projetado por vectorpocket / Freepik
	Projetado por Freepik
	Projetado por Photoroyalty / Freepik

CONFERÊNCIA DE INICIAÇÃO CIENTÍFICA

em Assuntos de Defesa

ES COM

DE FE SA

DECEX

CCOMGEX

DCT

A 1ª Conferência de Iniciação Científica em Assuntos de Defesa (CICAD.I.2018) tem como objetivos:

- contribuir para o avanço do conhecimento e aumento da produção científica em Defesa Nacional e em Ciências Militares; e

- estimular a interação entre os estabelecimentos de ensino civis e militares da Marinha, do Exército, da Aeronáutica e das Forças Auxiliares em assuntos afetos à Defesa Nacional e Ciências Militares.

PALAVRAS INICIAIS DO DIRETOR DE ENSINO DA ESCOLA DE COMUNICAÇÕES

É com muita satisfação que nos reunimos, neste auditório, para dar início a 1ª Conferência de Iniciação Científica em Assuntos de Defesa.

A Estratégia Nacional de Defesa (END), editada no ano de 2008, prevê, dentre outras diretrizes ligadas às Forças Armadas, o estreitamento do relacionamento entre o público militar e o público civil acadêmico, uma vez que Defesa Nacional não é um assunto especificamente militar, mas sim afeto a toda sociedade brasileira e, portanto, de interesse comum a todos os brasileiros.

A conjuntura atual, em seu cenário internacional, estimula o surgimento de temas de estudos afetos à Defesa Nacional e Segurança em contexto mais extensivo. Neste ínterim, inúmeros fenômenos de ordem mundial apontam para a necessidade do Poder Nacional fomentar a pesquisa em assuntos de Defesa. A título de exemplo, o terrorismo internacional, os crimes cibernéticos, a influência da guerra cibernética nos conflitos internacionais, bem como seu relacionamento com a Defesa e a sociedade são temáticas de interesse comum às nações e fomentam grandes debates no cenário internacional.

Cel Rodolfo Roque Salguero De La Vega Filho, Cmt EsCom

Nesse sentido, e em consonância com as diretrizes da END, Ministério da Defesa e Comando do Exército, que a Escola de Comunicações (EsCom) promove a criação da 1ª Conferência de Iniciação Científica em Assuntos de Defesa, convidando a sociedade acadêmica local a pensar juntos sobre os assuntos afetos à Defesa Nacional.

Dessa forma, encerro minhas palavras e declaro aberta a 1ª Conferência de Iniciação Científica em Assuntos de Defesa.

Sejam todos bem-vindos!

Geração de recursos no reaproveitamento de baterias de rádios militares: estudo de possibilidade e viabilidade

Ten Matheus Braga do Nascimento, pós-graduado do curso de Oficial de Comunicações

Cap Castellani, Asp Of Zanatta, Ten Matheus Braga e Sr Antônio Marcos

Ten De Paula, Sr Vítor Ossamu e o Professor Alexsandro Barreto

Estudo de Viabilidade de um enlace tático por tropodifusão em 440 Mhz

Cap Castellani, pós-graduado em Engenharia de Sistemas de Radiocomunicação pelo INATEL

Professor Plínio Ricardo Ganime Alves

Professor Alexsandro Barreto e Maj Dondoni

Itens de notícias relevantes

INFORMATIVO TÉCNICO

CIBERNÉTICA

RECRUDESCIMENTO DOS ATAQUES DE CRIPTOGRAFIA DE DADOS

Luiz Paulo Lopes dos Santos
Pós-Graduado, lato sensu, em Guerra Cibernética

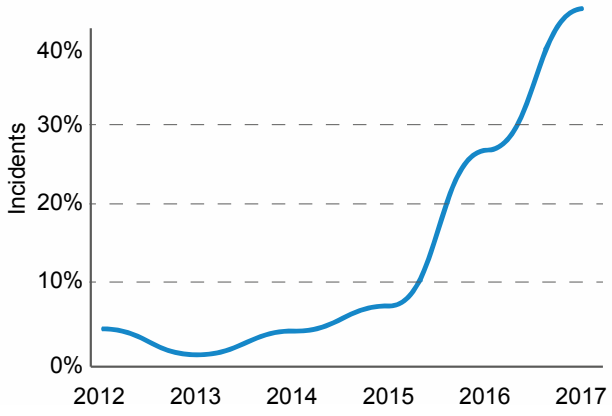
RESUMO: Um estudo recente de investigações sobre violação de dados revelou que o ransomware era a variedade mais prevalente de malware em 2017. De acordo com o "Relatório de Investigações de Violações de Dados (DBIR) de 2018 da Verizon", os profissionais de segurança identificaram o malware chamado ransomware em quase 40% dos incidentes de segurança que envolviam malware como uma de suas variedades de ataques. Esse tipo de ataque foi maior do que spywares, cavalos de Troia e outras formas de softwares mal-intencionados ao longo do ano. Os pesquisadores classificaram o ransomware como a quinta variedade de ação mais prevalente, com 787 incidentes, e observaram que o malware foi utilizado como uma tática em 30% dos eventos de segurança.

Palavras-chave: Phishing. Wannacry. Malware. Ransomware.

INTRODUÇÃO

Em maio de 2017, um ransomware, chamado de WannaCry, infectou mais de 200 mil computadores, fruto de um ataque que começou na Espanha e no Reino Unido, segundo HIGA (2017).

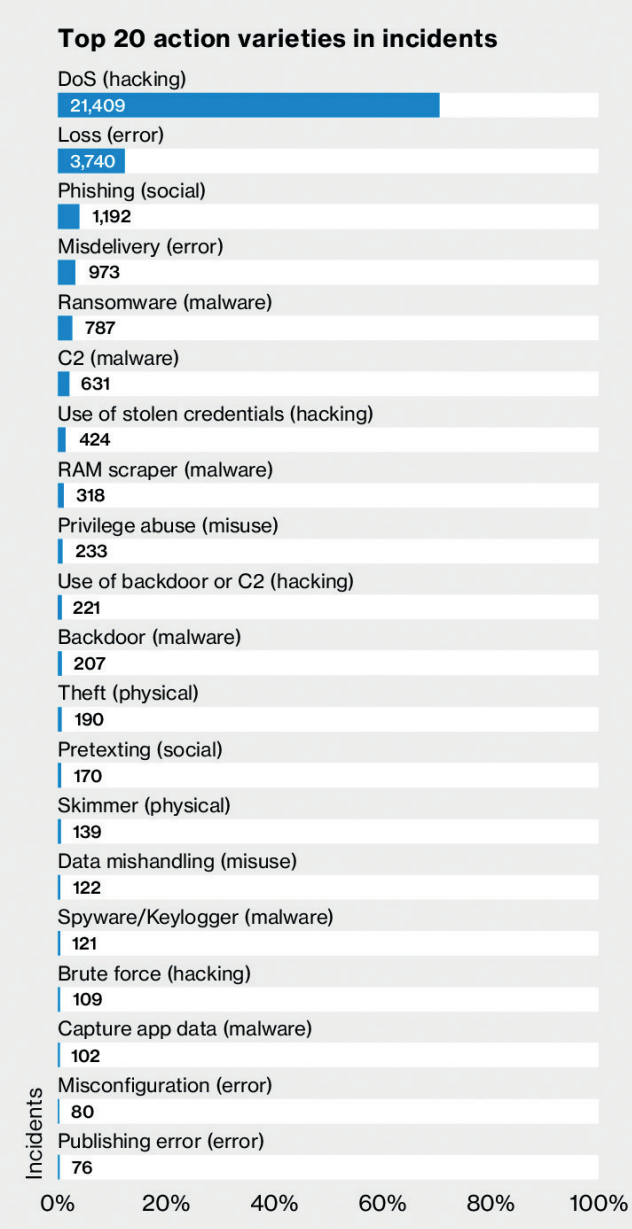
FIGURA 1 Ataque de rasomware nos últimos anos

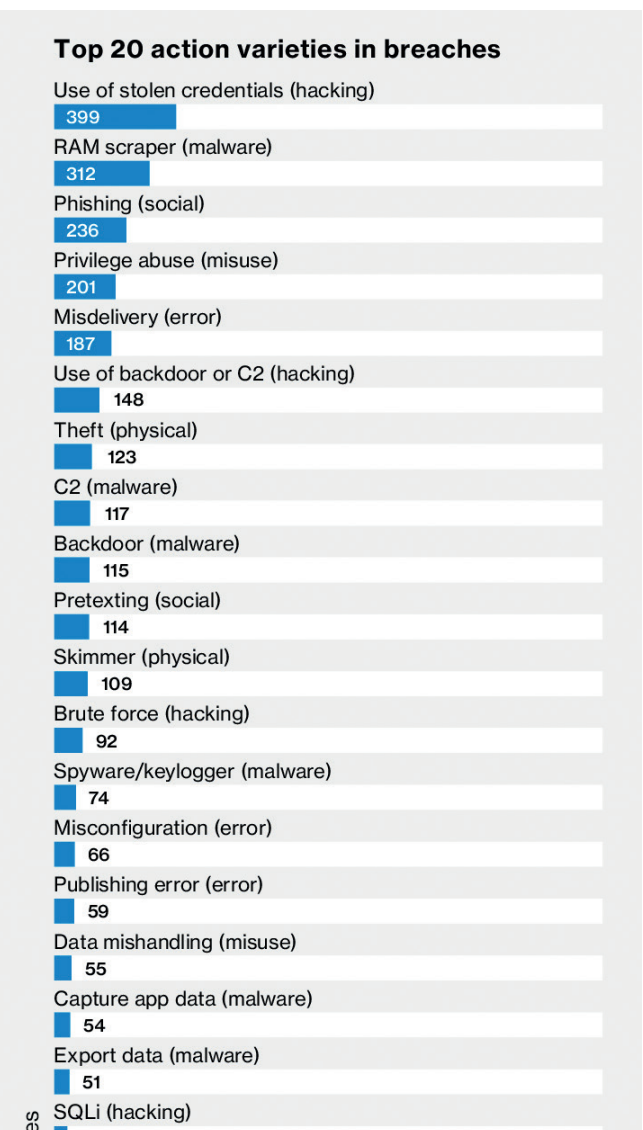


Fonte: DBIR 2018 – Verizon

Em 2018, de acordo com o relatório anual de informações da empresa Verizon, divulgado em 3/4/2018, podemos constatar que este tipo de malware ainda continua realizando seus ataques. A ameaça foi encontrada em 39% das violações de dados, o dobro em comparação com o ano passado, tornando-se a maior variedade de software malicioso.

FIGURA 2 As 20 principais variedades de ações em incidentes e violações





Fonte: DBIR 2018 - Verizon.

A 11ª edição do relatório analizou mais de 53.000 incidentes de segurança e 2.216 violações de 65 países. O relatório da Verizon aponta que os incidentes relacionados com o ransomware dobraram em relação a 2017.

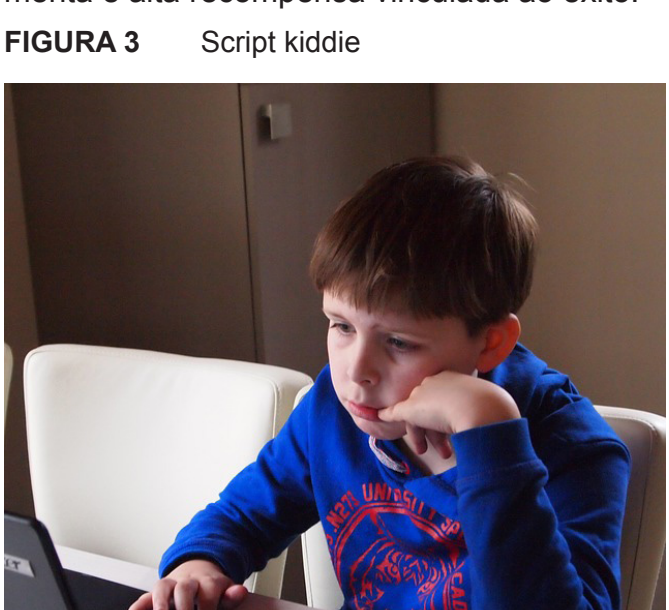
O motivo pelo qual estamos vendo essa incrível prevalência do ransomware sob as demais formas de ataques está vinculado ao grande valor agregado capturado pelo invasor (ZDNET, 2018).

Os atacantes não precisam usar rotinas ou sistemas complexos para que se consiga infectar um computador. Uma vez “solto” dentro da máquina, o malware trabalha sozinho para infectar o alvo original e quaisquer outros periféricos conectados a mesma rede.

Antes era difícil para hackers configurarem a criptografia necessária para implantar o ransomware, porém, hoje eles podem simplesmente comprar o software de que precisam.

Um Script Kiddie, nome atribuído de maneira depreciativa aos hackers inexperientes que procuram alvos fáceis para aplicar seus poucos conhecimentos técnicos (DORKSLAB, 2017), geralmente usa ferramentas prontas na internet para realizar ataques, já que o risco é baixo, dada a facilidade de obtenção da ferramenta e alta recompensa vinculada ao êxito.

FIGURA 3 Script kiddie



IMPACTO

O ransomware também começou a impactar os sistemas críticos de negócios, acarretando em demandas de resgate maiores, fazendo com que os cibercriminosos obtenham mais dinheiro por menos trabalho.

Hoje, com a facilidade da criptomoeda, qualquer ataque hacker bem-sucedido de criptografia de dados terá o pagamento irrastreável (CCMTECNOLOGIA, 2018).

As pequenas e médias empresas/lojas são as mais impactadas com uma criptografia de dados. A título de exemplo, o hospital de Câncer de Barretos teve todas as suas unidades de prevenção espalhadas pelo Brasil afe-

tadas como registrou o portal de notícias G1. GLOBO (2017).

Isso significa que uma empresa que tenha todo o seu histórico de consultas, pagamentos, contas, devedores e diversas informações criptografadas, caso não possua um sistema de backup salvo do ataque, terá perda total de seus sistemas.

E esse tipo de ataque está fazendo diversas vítimas ao redor do mundo, de acordo com o site ZDNET (2018).

Essas empresas são coagidas a pagarem o resgate com criptomoedas, mesmo não tendo garantias de que os dados serão, de fato, devolvidos (FANTÁSTICO, 2017).

Também temos problemas e impactos causados às pessoas que continuam sendo vítimas de ataques de engenharia social, segundo o relatório. O email continua a ser o principal ponto de entrada para malware, com 96% dos ataques chegando através de caixas de entrada.

As empresas também têm quase três vezes mais chances de serem violadas devido a ataques de engenharia social do que com vulnerabilidades reais, destacando a necessidade de educação cibernética contínua dos funcionários.

O relatório também apontou que 78% das pessoas não estão caindo no golpe do phishing, alguns aplicados pelas próprias empresas para testar o treinamento de seus funcionários como esclarece Olenick (2017), e ensina Stu (2016), onde o primeiro fala que a melhor defesa é o ataque, e afirma que envia e-mails falsos para seus próprios funcionários, para testar o treinamento oferecido pela empresa contra o ataque, e estas por sua vez podem focar seus esforços de educação anti-phishing em pequenos grupos de empregados.

CONCLUSÕES

O ransomware, quando atua contra indústrias da área de saúde, apresenta um dano potencial, ainda, imensurável se confrontado com outras áreas industriais de significativa relevância.

O surto ocorrido em maio de 2017, deixando 34% dos hospitais do Serviço Nacional de Saúde do Reino Unido inoperantes exemplifica bem a suscetibilidade a ataques de malware. Essas informações coadunam com o relatório da Verizon, onde os dados apontam que 85% de todas as variedades de malware atingem os serviços de saúde (NHS, 2018).

O mesmo relatório observou que as organizações médicas são obrigadas por regulamentos federais a relatar ataques de ransomware como violações de dados e não como risco de dados. Portanto, é impossível saber se os hospitais e outros centros de saúde são mais suscetíveis a ransomware do que as organizações de outros setores, pois esses setores relatam os ataques como riscos de dados.

O relatório cita, ainda, boas práticas que buscam atenuar e erradicar os efeitos, tais como a autenticação de dois fatores, correção de vulnerabilidades de software e realização de treinos contínuos de conscientização de segurança aos usuários.

Por fim, embora tenha-se percebido, no ano de 2017, inúmeros ataques de rasonware a uma diversidade de setores, pouco foi feito no período de um ano, pois o novo relatório aponta carência de conscientização sobre a segurança de dados. É imprescindível que ações efetivas sejam tomadas, desde a atualização dos sistemas e softwares de proteção locais até a contratação de serviços de salvaguarda de dados, monitoramento e resolução de incidentes.

RECRUDESCENCE DATA ENCRYPTION ATTACK

ABSTRACT. A RECENT STUDY OF DATA BREACH INVESTIGATIONS REVEALED THAT RANSOMWARE WAS THE MOST PREVALENT VARIETY OF MALWARE IN 2017. ACCORDING TO VERIZON'S "DATA VIOLATIONS INVESTIGATION REPORT (DBIR) 2018, SECURITY PROFESSIONALS HAVE IDENTIFIED THE MALWARE CALLED RANSOMWARE IN NEARLY 40% OF SECURITY INCIDENTS INVOLVING MALWARE AS ONE OF ITS VARIETIES OF ATTACKS. THIS TYPE OF ATTACK WAS GREATER THAN

spyware, Trojans and other forms of malicious software throughout the year. The researchers ranked ransomware as the fifth most prevalent action variety, with 787 incidents, and found that malware was used as a tactic in 30% of security events.

Keywords: Phishing. Wannacry. Malware. Ransomware.

REFERÊNCIAS

CCMTECNOLOGIA. Veja como o sequestro de dados afeta pequenas e médias empresas, 2018. Disponível em: < https://www.ccmtecnologia.com.br/blog/veja-como-o-sequestro-de-dados-afeta-pequenas-e-medias-empresas/> Acesso em: 10 Maio. 2018.

DORKSLAB. Os tipos de hackers, 12 junho 2017. Disponível em: < http://www.dorkslab.com.br/2017/06/os-tipos-de-hackers.html/> Acesso em: 11 Maio. 2018.

FANTASTICO. G1.GLOBO. Hackers pedem resgate em moedas virtuais como o bitcoin, 14 maio 2017. Disponível em: <http://g1.globo.com/fantastico/noticia/2017/05/hackers-pedem-resgate-em-moedas-virtuais-como-o-bitcoin.html>Acesso em: 11 Maio. 2018.

G1.GLOBO. Após ciberataque, Hospital de Câncer de Barretos estima 5 dias para normalizar atendimentos em todo o país, 27 março 2018. Disponível em: <https://g1.globo.com/sp/ribeirao-preto-franca/noticia/apos-ciberataque-hospital-de-cancer-de-barretos-estima-5-dias-para-normalizar-atendimentos-em-todo-o-pais.ghtml/> Acesso em: 11 Maio. 2018.

HIGA, PAULO. Ransomware WannaCry já infectou 200 mil computadores em 150 países, Janeiro 2017. Disponível em: <https://tecnoblog.net/214656/wannacry-ataque-disseminacao-150-paises/>. Acesso em: 10 Maio 2018.

NHS. Lessons learned review of the WannaCry Ransomware Cyber Attack, 01 fevereiro 2018. Disponível em: <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf/> Acesso em: 11 Maio. 2018.

OLENICK, DOUG. Top 5 anti-phishing training programs, 10 outubro 2017. Disponível em: <https://www.scmagazine.com/top-5-anti-phishing-training-programs/article/699119/> Acesso em: 11 Maio. 2018.

STU. How To Phish Your Employees, janeiro 2016. Disponível em: <https://www.knowbe4.com/resources/how-to-phish-your-employees/> Acesso em: 11 Maio. 2018.

TECHPRORESEARCH. Cybersecurity spotlight: The ransomware battle, Agosto 2016. Disponível em: <http://www.techproresearch.com/downloads/cybersecurity-spotlight-the-ransomware-battle/>. Acesso em: 04 março 2018.

VERIZON ENTERPRISE. 2018 Data Breach Investigations Report, 09 Abril 2018. Disponível em: <https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf>. Acesso em: 10 Maio 2018.

ZDNET. Atlanta, hit by ransomware attack, also fell victim to leaked NSA exploits, 27 março 2018. Disponível em: <https://www.zdnet.com/article/atlanta-hit-by-ransomware-attack-also-fell-victim-to-leaked-nsa-exploits/> Acesso em: 06 Março. 2018.

ZDNET. Cybercriminals switching from ransomware to mining malware attacks, 06 março 2018. Disponível em: <https://www.zdnet.com/video/cryptocurrency-mining-malware-now-as-lucrative-as-ransomware-for-hackers/> Acesso em: 04 Março. 2018.

O autor é graduado em Ciências Militares pela AMAN e pós-graduado em Guerra Cibernética pelo CIGE. Atualmente, exerce a função de Chefe de Seção de Ensino a Distância na Escola de Comunicações e pode ser contactado pelo email luizpaulo.santos@eb.mil.br

ITENS DE NOTÍCIAS RELEVANTES

INFORMATIVO TÉCNICO

CIÊNCIA E TECNOLOGIA

PROJETO DE LOUSA INTERATIVA UTILIZANDO UMA WEBCAM E LASER POINT

Fernando Henrique Castellani[1], Carlos Eduardo Agnelo da Rocha[2]
Mestre em Ciências Militares[1]; Graduado em Ciências Militares[2].

RESUMO: Este artigo foi idealizado com o propósito de apresentar uma proposta de melhoramento das ferramentas utilizadas na atividade de instrução. É sabido que o Exército Brasileiro (EB) tem algumas restrições orçamentárias, sobretudo para aquisição de material permanente. Esse estudo aponta uma solução para utilização de uma ferramenta de apoio à atividade de instrução com um custo de implementação bastante reduzido. Além da versatilidade, essa proposta se mostra como uma alternativa adequada aos objetivos aos quais ela se propõe. Capaz de proporcionar a interação com a projeção de imagens, de modo similar a outros materiais disponíveis no comércio, porém com algumas vantagens que vão desde a instalação até a desnecessidade de obtenção de licenças para o funcionamento do produto. Assim sendo, a alternativa aqui exposta se reveste de utilidade haja vista suas características sabidamente favoráveis, seja no aspecto prático, seja no econômico.

Palavras-chave: Exército. Interação. Projeção. Vantagens. Prático.

INTRODUÇÃO

A ideia de introduzir no ambiente de instrução uma técnica diferenciada para transmissão do conhecimento não apenas tem por objetivo reduzir o gasto com o material empregado mas também diversificar e inovar em ferramentas que irão contribuir para que a aprendizagem ocorra de modo satisfatório.

Segundo o Manual do Instrutor, os meios auxiliares são os recursos utilizados pelo instrutor e pelos discentes para a organização e condução do processo ensino-aprendizagem e que auxiliam a comunicação.

A comunicação, ou ainda, a transmissão do conhecimento com mais alcance e mais efetividade é a razão de ser do presente trabalho.

1 METODOLOGIA

O desenvolvimento do trabalho ocorrerá de forma documental, mostrando um passo a passo a ser seguido de modo a implementar a ferramenta que substitui uma lousa interativa convencional. As fontes serão softwares, programas e manuais encontrados na internet e que relacionam-se com o assunto. Os procedimentos a serem adotados consistem numa sequência de eventos que podem ser replicados em qualquer ambiente de ensino desde que obedecidos certos requisitos e configurações, aqui apresentados.

2 RESULTADO E DISCUSSÃO

2.1 VISÃO GERAL

O software Webcam Whiteboard possui a capacidade de rastrear, em uma tela, um ponto de luz visível ou infravermelho, através de uma webcam, associando o deslocamento deste ponto de luz ao movimento do mouse, possibilitando a criação de uma Lousa Interativa de baixo custo. A utilização deste sistema possibilita algumas vantagens quando comparado ao Smart Board convencional, como:

- pode ser levado facilmente de um local para outro;
- fácil configuração, necessitando de cerca de 10 minutos para estar pronto para operar;
- baixo custo (aproximadamente R$ 150,00);
- fácil utilização;

- possui praticamente as mesmas funcionalidades que o Smart Board convencional;

- sem necessidade do pagamento de licenças de software.

2.2 REQUISITOS

Para o perfeito funcionamento do sistema, há necessidade do software principal, um projetor multimídia, uma tela de projeção, uma webcam e um laser point verde. O computador utilizado deverá possuir o Windows XP ou superior.

A webcam deve ter uma resolução real de 1.3 mega pixel e uma taxa de 30 quadros por segundo ou frames per second (fps), assim como possibilitar o ajuste manual de exposição à Luz.

A webcam utilizada neste trabalho foi a “Matrix EasyCam 1.3Mp” da marca “Fortrek”.

Webcam Fortrek

Os laser points comuns, de cor vermelha, não possuem potência suficiente para sensibilizar a webcam.

Logo, para que o experimento ocorra de modo satisfatório, o laser point deve ser de cor verde, assim como possuir uma potência de aproximadamente 200 mW, como mostrado na figura seguinte:

Laser Verde de 200 mW

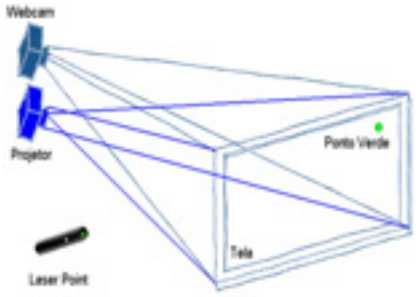
2.3 INSTALAÇÃO

Para a execução do software o computador deve possuir o JAVA versão 1.6 ou superior. Caso ocorra a necessidade de instalar o software, pode-se realizar o download na página da empresa através do endereço a seguir: http://www.java.com/pt_BR/download/windows_ie.jsp?locale=pt_BR&host=www.java.com.

A webcam deve ser instalada no computador onde o software estará sendo utilizado. Como cada webcam possui um instalador diferente, este passo não será abordado aqui.

A webcam deverá ser posicionada em um local que proporcione uma visão de toda a tela onde está sendo realizada a projeção.

Um dos melhores locais para posicionar a webcam é em cima do Projetor Multimídia, proporcionando uma visão semelhante à mostrada na figura a seguir:



Posição da Webcam

Pode-se também posicionar a webcam em outros locais, contanto que a mesma “enxergue” a tela e o ponto luminoso verde produzido pelo laser.

2.4 CONFIGURAÇÃO

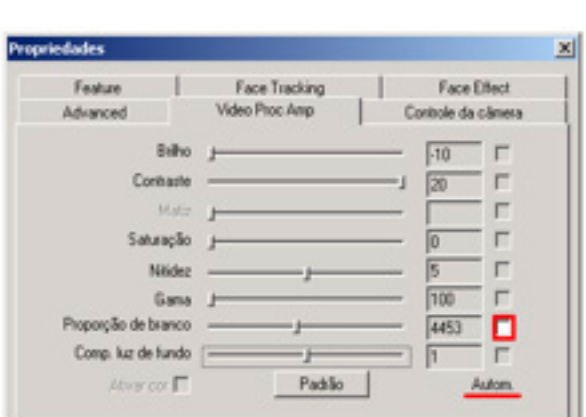
A seguir será apresentada uma proposta para configuração da webcam e do software.

2.4.1 Webcam

Antes de iniciar o uso do software, deve-se configurar a webcam. Para tanto, deve-se acessar as configurações da webcam, o que pode ser feito através do programa AMCAP, instalado com a maioria das webcams

disponíveis no mercado.

As opções de configuração devem ficar semelhantes ao mostrado na figura abaixo:



Configuração dos controles

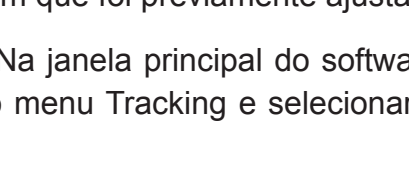
Dessa forma, brilho, saturação, e gama devem ser reduzidos ao mínimo; o contraste deve ser aumentado para o máximo e a nitidez, componente de luz de fundo e proporção de branco podem ficar na posição central. É muito importante desativar a opção de controle automático, pois isto causará problemas durante a operação do software.

Outra opção de ajuste obrigatório é a exposição à luz, que deve ficar em manual para que a luz seja captada pela webcam.

2.4.2 Software

Ao iniciar o Webcam WhiteBoard, será perguntado qual o dispositivo a ser utilizado como captura de vídeo, devendo-se selecionar a webcam que foi previamente ajustada.

Na janela principal do software, deve-se ir ao menu Tracking e selecionar a opção Infrared:



Webcam whiteboard

Apesar do laser trabalhar no espectro de luz visível (Color) e não no infravermelho, o algoritmo do software apresenta melhor desempenho com a opção Infrared selecionada.

No menu cursor deve-se verificar se a opção Track and Click está selecionada.

Na janela settings deve-se ajustar inicialmente o Infrared-Sensitivity para 20, ajustar o clique do mouse para Slow, selecionar o Vídeo para Type=RGB24 Width=640 Height=480 FPS=30.000, e clicar em Apply.

Nesse ponto, deve-se observar qual é a velocidade de processamento de quadros por segundo ou frames per second (fps) em que o software está conseguindo trabalhar, observando-se esta informação na janela principal.

A velocidade deve ficar entre 29 e 31 fps. Caso isso não aconteça, deve-se realizar algumas verificações.

O principal responsável por este problema é uma webcam de baixa qualidade, que não consegue produzir imagens de 640x480 pixels a uma velocidade de 30 fps. Neste caso, sugere-se substituir a webcam.

Outro motivo pode ser a ligação a uma porta USB que não esteja em perfeitas condições. Nesse caso, pode-se trocar a porta utilizada. É interessante verificar se a conexão é USB 2.0. Não é aconselhável utilizar HUBs USB.

O cabo USB que liga a webcam ao computador também não deve exceder 8 metros, sob pena de diminuir o fps ou mesmo impedir que a webcam funcione.

O computador também pode ser o motivo, caso esteja executando vários processos ao mesmo tempo, o que fará com que a execução do software fique mais lenta. Nesse caso, podem ser desativados programas que não estão sendo utilizados, fechar janelas desnecessárias ou até mesmo desativar temporariamente o software antivírus.

Outra opção é fazer com que o Windows priorize o desempenho. Para isso, basta clicar com o botão direito do mouse sobre o

ícone do Meu Computador, e acessar propriedades. Na Aba Avançado, clicar no botão configurações no item Desempenho, e na janela que abrir, selecionar Ajustar para obter um melhor desempenho.

Caso nenhuma dessas opções surta efeito pode-se tentar utilizar o software em outro computador, que possua uma configuração melhor (processador mais rápido, maior quantidade de memória RAM). Recomenda-se que o computador utilizado tenha um processador de 3 GHz ou equivalente, com 1 GB de memória RAM.

Deve-se depois acessar o menu Extras e selecionar a opção Tracking Monitor, o que mostrará a tela onde o algorítmo do software está detectando o ponto luminoso criado pelo laser point ao atingir a tela

Se as configurações estiverem corretas, será detectado apenas 1 (um) Blob (ponto luminoso detectado pelo algoritmo do software). Caso as configurações não estejam adequadas, o software irá detectar vários Blobs, provenientes de outros pontos que estão com a luminosidade mais elevada.

Nesse caso, deve-se manter a janela Traking Monitor aberta e abrir a janela Settings, ajustando o Infrared-Sensitivity para um valor que produza apenas um único Blob quando o laser for acionado e apontado para a tela de projeção.

Sempre deve-se deixar este ajuste no mínimo possível para que seja feita a detecção apenas do Blob produzido pelo laser, pois ao aumentar a sensibilidade, corre-se o risco de que a luminosidade local acabe produzindo falsos blobs, principalmente quando a projeção estiver trabalhando com imagens em cores claras como o branco, por exemplo.

Feitos os ajustes, pode-se iniciar a calibragem da área onde o algoritmo irá considerar como sendo o “Quadro Branco” ou Lousa Interativa, bastando para isso clicar no botão Calibrate, na janela principal.

2.5 UTILIZAÇÃO

Finalizados os ajustes tanto da webcam quanto do software, já é possível utilizá-lo, bastando clicar com o mouse no botão Start da janela principal.

Desse ponto em diante, toda vez que o laser point for direcionado para a tela de projeção e acionado, o mouse acompanhará o movimento do ponto luminoso gerado pelo laser. Agora, o mouse é controlado pelo laser point.

Nas apresentações de Power Point, os slides podem ser avançados pelo simples acionamento do laser na tela de projeção, o que equivale ao clique do mouse.

Pode-se também fazer uso da barra de ferramentas presente no Power Point e em outros softwares de apresentações, aumentando as funcionalidades do laser.

CONCLUSÃO

Ante o exposto, verifica-se que a alternativa apresentada neste trabalho se mostra como uma opção economicamente viável além de caracterizar-se como uma medida de simples adoção haja vista não requerer muitos insumos.

Por fim, sua utilização é recomendada para suprir a necessidade de um recurso didático versátil de apoio à atividade de ensino/instrução nas organizações militares, com um baixo custo e elevado grau de confiabilidade.

PROYECTO LOUSA INTERACTIVA UTILIZANDO UNA WEBCAM Y LÁSER POINT

RESUMEN. ESTE ARTÍCULO FUE PENSADO CON EL PROPÓSITO DE PRESENTAR UNA PROPUESTA DE MEJORA DE LAS HERRAMIENTAS UTILIZADAS EN LA ACTIVIDAD DE INSTRUCCIÓN. ES SABIDO QUE EL EJÉRCITO BRASILEÑO (EB) TIENE ALGUNAS RESTRICCIONES DE PRESUPUESTOS, SOBRE TODO PARA LA ADQUISICIÓN DE MATERIAL PERMANENTE. ESTE ESTUDIO SEÑALA UNA SOLUCIÓN PARA UTILIZAR UNA HERRAMIENTA DE APOYO A LA ACTIVIDAD DE INSTRUCCIÓN CON UN COSTO DE IMPLEMENTACIÓN BASTANTE REDUCIDO. ADEMÁS DE LA VERSATILIDAD, ESTA PROPUESTA SE PRESENTA COMO UNA ALTERNATIVA ADECUADA A LOS RETOS

que se proponem. Capaz de proporcionar la interacción con la proyección de imágenes, de modo similar a otros materiales disponibles en el comercio, pero con algunas ventajas que van desde la instalación hasta la falta de necesidad de obtener licencias para el funcionamiento del producto. Por lo tanto, la alternativa aquí expuesta se reviste de utilidad teniendo en cuenta sus características seguramente favorables, sea en el aspecto práctico, sea en el económico

Palabras-clave: Ejército. interacción. proyección. ventajas. práctico.

REFERÊNCIAS

BRASIL. Exército. Estado-Maior. T 21-250: Manual do Instrutor. 3. Ed. Brasília, DF, 1997.

Software Click Aid: Polital Enterprises. Disponível em: http://www.polital.com/assist/ Acesso em: 16 de junho de 2018.

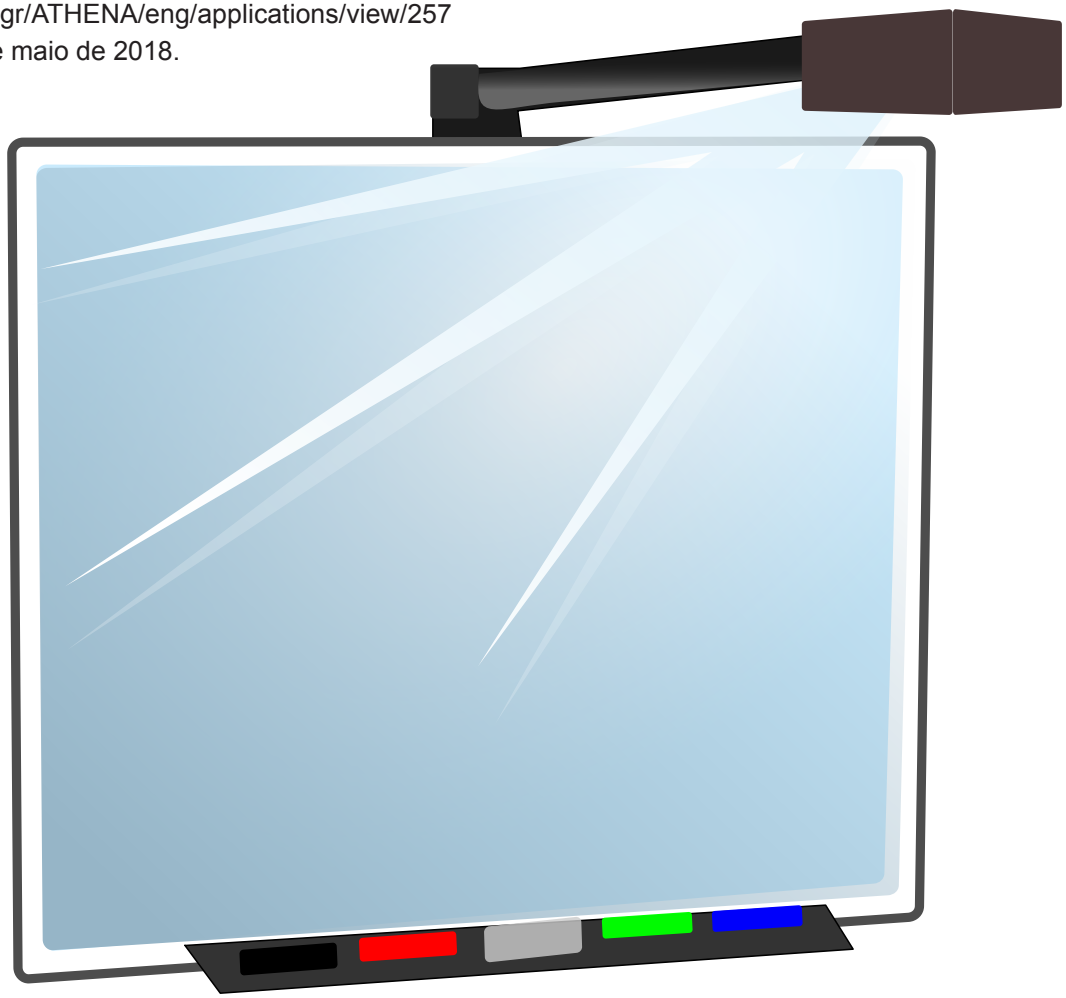
Software Free Virtual Keyboard: Comfort Software Group Disponível em: https://free-virtual-keyboard.softonic.com.br/ Acesso em: 10 de junho de 2018.

Software Mouse Click: Uri Fridman Disponível em: http://access.uoa.gr/ATHENA/eng/applications/view/257 Acesso em: 16 de maio de 2018.

Software Webcam Whiteboard: Eduard Metzger. Disponível em: http://www.webcam-whiteboard.com. Acesso em: 5 de maio de 2018.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) e mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO). É pós-graduado em Telecomunicações pelo Instituto Nacional de Telecomunicações (INATEL). Atualmente, exerce a função de instrutor no Centro de Instrução de Guerra Eletrônica (CIGE) e pode ser contactado pelo email fhcastellani@gmail.com.

O co-autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) e pós-graduado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO). Atualmente, exerce a função de instrutor na Escola de Comunicações (EsCom) e pode ser contactado pelo email carlos109eduardo@gmail.com.



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