ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP ART MARCELO EDUARDO DE SOUZA CONCEIÇÃO

ATAQUES CIBERNÉTICOS PERPETRADOS NA ATUALIDADE E OS POSSÍVEIS IMPACTOS PARA AS OM DO EXÉRCITO BRASILEIRO

Rio de Janeiro
2017

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP ART MARCELO EDUARDO DE SOUZA CONCEIÇÃO

ATAQUES CIBERNÉTICOS PERPETRADOS NA ATUALIDADE E OS POSSÍVEIS IMPACTOS PARA AS OM DO EXÉRCITO BRASILEIRO

Trabalho acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares

Rio de Janeiro
2017

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DECEx - DESMil
ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS
(EsAO/1919)

DIVISÃO DE ENSINO / SEÇÃO DE PÓS-GRADUAÇÃO

FOLHA DE APROVAÇÃO

Autor: **Cap Art MARCELO EDUARDO DE SOUZA CONCEIÇÃO**

Título: **ATAQUES CIBERNÉTICOS PERPETRADOS NA ATUALIDADE E OS POSSÍVEIS IMPACTOS PARA AS OM DO EXÉRCITO BRASILEIRO**

Trabalho Acadêmico, apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito parcial para a obtenção da especialização em Ciências Militares, pós-graduação universitária lato sensu.

APROVADO EM _____/_____/_____CONCEITO: _____

BANCA EXAMINADORA

Membro	Menção Atribuída
_____ **XXXXXXXXXXXXXXXX- TC** Cmt Curso e Presidente da Comissão	
_____ **XXXXXXXXXXXXXXXX Cap** 1º Membro	
_____ **XXXXXXXXXXXXXXXX - Maj** 2º Membro e Orientador	

_____
MARCELO EDUARDO DE SOUZA CONCEIÇÃO – Cap
Aluno

ATAQUES CIBERNÉTICOS PERPETRADOS NA ATUALIDADE E OS POSSÍVEIS IMPACTOS PARA AS OM DO EXÉRCITO

Marcelo Eduardo de Souza Conceição

RESUMO

No século XXI, com o surgimento da rede mundial de computadores, uma nova ameaça se apresenta no cenário bélico internacional: a guerra cibernética. Esse novo vetor se torna cada vez mais presente com o aumento da capacidade computacional e a forte necessidade da tecnologia da informação por parte de governos e empresas. O Brasil, desde 2012, busca se adequar a esse novo cenário com a criação do Centro de Defesa Cibernética e com políticas de segurança da informação. A fim de verificar de que modo as Organizações Militares do Exército Brasileiro, em particular da 9ª Bda Inf Mtz, estão preparadas para se defender dos vetores cibernéticos ofensivos, o estudo focou no nível de conscientização do público interno, particularmente dos capitães que serviram nas referidas OM nos últimos 3 anos, no que diz respeito à utilização dos recursos de tecnologia da informação em sua Unidade, uma vez que o recurso humano é o elo mais fraco na estratégia de segurança cibernética de qualquer órgão, porém, quando bem instruídos, se tornam a defesa mais forte.

Palavras-chave: Ataque cibernético. 9ª Bda Inf Mtz. Conscientização do público interno. Recurso humano. Defesa cibernética.

ABSTRACT

In the 21st century, with the emergence of the world wide web, a new threat presents itself in the international war scene: cyber warfare. This new vector becomes increasingly present with the increase of computational capacity and the strong need of information technology by governments and companies. Brazil, since 2012, seeks to adapt to this new scenario with the creation of the Center for Cyber Defense and information security policies. In order to verify how the Military Organizations of the Brazilian Army, in particular the 9th Bda Inf Mtz, are prepared to defend themselves against offensive cybernetic vectors, the study focused on the level of awareness among the internal public, particularly of the captains who served in these OM in the last 3 years, regarding the use of information technology resources in his Unit, since human resources are the weakest link in the cybersecurity strategy of any organ, but when well instructed, they become the strongest defense.

Keywords: Cyber attack. 9th Bda Inf Mtz. Awareness of the internal public. Human resource. Cyber defense.

1 INTRODUÇÃO

O avanço da computação e da rede mundial de computadores (internet) trouxe uma série de benefícios às organizações e pessoas. Os processos se tornaram mais rápidos e eficientes, em todas as etapas. Entretanto, junto com os benefícios das soluções de tecnologia da informação, vieram, também, os *malwares*: códigos maliciosos criados para diversas finalidades que se aproveitam de falhas nos sistemas e aplicações para realizar a ação que foi proposta.

A grande ameaça dos malwares advém dos crackers, indivíduos com grande expertise na área cibernética que utilizam seus conhecimentos para realizar atividades maliciosas nas redes de computadores a fim de obter vantagens individuais.

Além disso, no cenário bélico, países como Estados Unidos, Inglaterra, China, Alemanha e Japão criaram, dentro de sua estrutura militar, um corpo destinado à atuar no cenário cibernético.

Nesse contexto, o Brasil e o Exército Brasileiro tem sido um dos principais alvos de ataques cibernéticos nos últimos anos.

1.1 PROBLEMA

O cenário bélico internacional tem sofrido diversas modificações, durante o passar dos anos, desde os conceitos táticos aplicados nas batalhas até as estratégias para se vencer uma guerra. Essa evolução sempre foi marcada com o advento de novas tecnologias aplicada ao combate.

O advento da pólvora, o surgimento das aeronaves e as bombas de fissão nuclear foram algumas das tecnologias determinantes no século XX para que uma nação se impusesse no combate frente às demais.

Entretanto, ainda no final do século XX, em um momento em que os governos não previam a força que o poder computacional e a rede mundial de computadores teriam no cenário internacional do século XXI, surge o termo de Guerra Cibernética, criado pelo autor norte-americano William Gibson, na obra de ficção *Neuromancer* em 1984.

Após os atentados às torres gêmeas nos Estados Unidos da América, de 11 de setembro de 2001, a Segurança Cibernética passou a ganhar maior importância por diversos países.

Anos mais tarde, com a rápida evolução computacional e da internet, os conceitos sobre a Guerra Cibernética foram mais explorados até ser compreendida

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 da informação". (CANONGIA e MANDARINO, p. 2009).

O Brasil, preocupado com esse novo vetor de combate e com a segurança das informações trafegadas nos órgãos federais, publicou em 2006 o Decreto nº 5.772 com a criação do Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), o qual, dentre suas atribuições, possui a de orientar a implementação de ações de segurança da informação e comunicações, inclusive as de segurança cibernética, no âmbito da administração pública federal.

De acordo com a PwC, em seu artigo sobre a evolução de ameaças e ataques cibernéticos de março de 2015, as ameaças e crimes cibernéticos organizados e direcionados preocupam países, sociedades e organizações. Exposições de informações críticas e incidentes de segurança em infraestrutura continuam crescendo no mundo inteiro.

Dessa forma, verifica-se a necessidade de estudar as formas de prevenção a ataques cibernéticos para que as Organizações Militares do Exército Brasileiro possam se defender dessa nova ameaça.

Neste sentido, a presente investigação pretende verificar em que medida as OM do Exército Brasileiro, em particular as OM da 9ª Brigada de Infantaria Motorizada (Brigada Escola), estão preparadas para se defender de ataques cibernéticos.

1.2 OBJETIVOS

A fim de verificar de que modo asUnidades do Exército Brasileiro estão preparadas para se defender dos vetores cibernéticos ofensivos, o presente estudo pretende, como objetivo geral, verificar o nível de conscientização dos oficiais do Exército quanto aos esforços de prevenção a ataques cibernéticos.

Para viabilizar a consecução do objetivo geral de estudo, foram formulados os objetivos específicos, abaixo relacionados, que permitiram o encadeamento lógico do raciocínio descritivo apresentado neste estudo:

a. Identificar os ataques cibernéticos, do cenário atual, que possam gerar danos às Organizações Militares do Exército Brasileiro;

b. Descrever as melhores formas de prevenção a ataques cibernéticos.

c. Identificar, a partir da opinião dos Capitães que serviram nos últimos 3 anos da 9ª Brigada de Infantaria Motorizada, o grau de conscientização sobre ações de prevenção a ataques cibernéticos; e

d. Identificar as possíveis soluções para aumentar o grau de conscientização dos militares sobre ações de prevenção a ataques cibernéticos;

1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

O aumentocrescente de ataques cibernéticos a empresas, órgãos governamentais e cidadãos do mundo inteiro ameaçam a privacidade e a economia mundial. Exposições de informações críticas e incidentes de segurança em infraestrutura continuam crescendo e atinge todos os segmentos, afirma a pesquisa de Março de 2015 da PricewaterhouseCoopers(PwC).

As informações tratadas no âmbito das Organizações Militares do Exército Brasileiro carecem de cuidados para que sejam disseminadas apenas para o público alvo que se destina. Muitos dados relativos à pessoal, operacionalidade, material e atividades devem ser tratados com rígida segurança para que não sejam levadas a conhecimento público ou de pessoas mal intencionadas.

A maior parte desses dados trafegam por meios de tecnologia da informação do Exército,por meio de aplicações hospedadas em servidores locais nas próprias Organizações Militares. Dessa forma, há necessidade de que se realize gestões de segurança da informação a fim de que medidas sejam adotadas de forma que dificultem, ao máximo, ataques cibernéticos perpetrados em sua estrutura de TI.

A pesquisa da PwC indica, também, que os esforços de prevenção envolvem um conjunto de ações, entre elas, a conscientização das pessoas e a implantação de soluções tecnológicas avançadas, além de uma estratégia de segurança cibernética que assegure maior resiliência em caso de ataque.

Dentro desse contexto, se faz necessária uma pesquisa a fim de conhecer o grau de conscientização dos militares do Exército Brasileiro acerca do assunto cibernético a fim de se conhecer qual o panorama atualde nossos recursos humanos.

O analista Luciano Barreto, da superintendência de tecnologia da informação da comissão de valores mobiliários alerta, em seu estudo, que algumas pessoas

não tem o cuidado necessário para evitar ser alvo de um ataque cibernético. Elas, enquanto andam na rua, têm o cuidado de não circular por certos lugares, porém, na internet, o comportamento nem sempre é o mesmo. E, por consequência disso, acabam sendo vítimas de ataques, inclusive quando estão em ambiente corporativo.

A empresa de consultoria Willis Towers Watson, indica em seu estudo sobre o risco cibernético, que no caso no *malware* WannaCry, ataque cibernético de grande escala perpetrado em 2017 que causou prejuízos de bilhões de dólares a diversas empresas e organizações por todo o planeta, a ativação foi iniciada através de e-mails de *phishing* (e-mails maliciosos com objetivo de roubar informações e dados pessoais por meio de mensagens falsas). Com isso, demonstra-se que os recursos humanos são o elo mais fraco na estratégia de segurança cibernética de qualquer empresa, porém, quando bem instruídos, se tornam a defesa mais forte.

Dentro desse contexto, o presente estudo se justifica por promover um conhecimento sobre a situação atual da consciência dos recursos humanos do Exército Brasileiro acerca do assunto cibernético.

O trabalho pretende, ainda, confeccionar uma cartilha de segurança da informação com informações úteis a fim de serem distribuídas nas OM e, dessa forma, aumentar a conscientização dos militares sobre o tema em questão.

2 METODOLOGIA

Para colher subsídios que permitissem formular uma possível solução para o problema, o delineamento desta pesquisa contemplou leitura analítica e fichamento das fontes, questionários e discussão de resultados.

Quanto à forma de abordagem do problema, utilizaram-se, principalmente, os conceitos de pesquisa **quantitativa**, pois as referências numéricas obtidas por meio dos questionários foram fundamentais para a compreensão das necessidades dos militares.

Quanto ao objetivo geral, foi empregada a modalidade **exploratória**, tendo em vista o pouco conhecimento disponível, notadamente escrito, acerca do tema, o que exigiu uma familiarização inicial, materializada pela pesquisa bibliográfica e seguida de questionário para uma amostra sobre o assunto.

2.1 REVISÃO DE LITERATURA

O delineamento da pesquisa iniciou-se com a definição de termos e conceitos, a fim de viabilizar a solução do problema de pesquisa, sendo baseada em uma revisão de literatura dos últimos três anos. Essa delimitação baseou-se na necessidade de atualização do tema, visto que o assunto em questão se encontra em constante evolução e a grande preocupação com o tema iniciou-sehá menos de uma década.

Foi realizada uma pesquisa sobre os tipos de ataques cibernéticos da atualidade e a influência da conscientização dos recursos humanos na proteção corporativa contra ataques cibernéticos, utilizando as palavras-chave recursos humanos, segurança da informação, conscientização, influência e ataques cibernéticos, juntamente com seus correlatos em inglês, em sítios eletrônicos de procura na internet.

a. Critério de inclusão:

- Estudos ematérias jornalísticas que apresentem os ataques cibernéticos perpetrados nos últimos 3 anos.

- Estudos publicados em português ou inglês, relacionados à influência da conscientização dos recursos humanos na proteção contra ataques cibernéticos;

- Estudos que indiquem os conhecimentosque os recursos humanos a fim de se proteger de ataques cibernéticos

b. Critério de exclusão:

- Estudos que abordem apenas tecnologias de softwares/hardwares para aumentar a capacidade de proteção cibernética; e

- Estudos cujo foco central não tenham relação direta com a conscientização dos recursos humanos.

2.2 COLETA DE DADOS

Na sequência do aprofundamento teórico a respeito do assunto, o delineamento da pesquisa contemplou a coleta de dados pelo seguintemeio: questionário.

2.2.1 Questionário

A amplitude do universo foi estimada a partir do efetivo de oficiais que serviram na 9ª Brigada de Infantaria Motorizada (Brigada Escola) nos últimos três anos. O estudo foi limitado particularmente aos capitães, que já serviram na 9ª

Brigada, já que os mesmos possuem uma visão mais completa dos militares que compõe as subunidades e, portanto, vivenciaram a forma como os militares subordinados interagiam com os equipamentos ligados na rede das Organizações Militares.

Dessa forma, utilizando-se dados obtidos no banco de dados da Diretoria Geral de Pessoal (DGP), a população a ser estudada foi estimada em cerca de 100 militares. A fim de atingir uma maior confiabilidade das induções realizadas, buscou-se alcançar uma amostra significativa, utilizando como parâmetros o nível de confiança igual a 90% e erro amostral de 10%. Nesse sentido, a amostra dimensionada como ideal (n_{ideal}) foi de 33.

Dessa feita, foram distribuídos questionários, via formulário do Google, para cerca de 80capitães do EB que serviram nos últimos três anos em Organizações Militares da 9ª Brigada de Infantaria Motorizada.

O efetivo acima foi obtido considerando 150% da amostra ideal prevista (n_{ideal}=33), utilizando-se como N o valor de 100 militares.

A sistemática de distribuição dos questionários ocorreu de forma indireta (formulário do google) entretanto, devido a diversos fatores, somente 32 respostas foram obtidas, não havendo necessidade de invalidar nenhuma por preenchimento incorreto ou incompleto.

A partir do n_{ideal} (33), depreende-se que o tamanho amostral obtido (n=32) foi inferior ao desejado para o tamanho populacional dos potenciais integrantes da amostra, no entanto não inviabiliza, tampouco reduz a relevância desta pesquisa, haja vista a especialização da amostra.

Foi realizado um pré–teste com 5 capitães-alunos da Escola de Aperfeiçoamento de Oficiais (EsAO), que atendiam aos pré-requisitos para integrar a amostra proposta no estudo, com a finalidade de identificar possíveis falhas no instrumento de coleta de dados. Ao final do pré-teste, não foram observados erros que justificassem alterações no questionário e, portanto, seguiram-se os demais de forma idêntica.

3 RESULTADOS E DISCUSSÃO

A pesquisa sobre o grau de conscientização dos militares sobre a prevenção de ataques cibernéticos às infraestruturas das Organizações Militares do Exército

Brasileiro, de uma forma inicial e superficial, mostrou-se satisfatória. Na pergunta inicial, foi questionado se o militar se preocupa com a segurança dos meios de TI de sua Organização Militar, e o militar tinha duas opções de resposta, como mostra a tabela abaixo:

Grupo / Resposta Obtida	Amostra	
	Valor absoluto	Percentual
Sim, entendo que devo fazer minhaparte para aumentar a segurançacibernética de minha OM	30	93,8%
Não, acredito que os sistemas devemser suficientemente seguros e que eu,como usuário, não devo mepreocupar com isso.	2	6,2%
TOTAL	32	100,0%

Fonte: O autor

Dos questionários recebidos, verificamos que 93,8% dos militares tem a consciência de que têm um papel importante para aumentar a segurança cibernética de sua Organização Militar, e que a responsabilidade não é somente dos gestores de TI e dos sistemas computacionais de segurança.

A partir dessa pergunta, o questionário começa a abordar aspectos pessoais de segurança para verificar se o militar tem um conhecimento básico sobre segurança cibernética e se ele realiza ações preventivas contra ataques cibernéticos.

Dessa forma, foi questionado se o militar alguma vez já havia conectado seu notebook, netbook ou tablet na rede de sua OM. As respostas obtidas foram as seguintes:

Grupo / Resposta Obtida	Amostra	
	Valor absoluto	Percentual
Sim, muitas vezes.	16	50,0%
Sim, poucas vezes.	4	12,5%
Não.	12	37,5%
TOTAL	32	100,0%

Fonte: O autor

É possível identificar sobre esse item no questionário que a maioria dos militares (62,5%) utilizam ou já utilizaram seus dispositivos pessoais em sua

Organização Militar. Isso é um fato preocupante, já que na rede da Organização Militar só se deve utilizar os ativos de TI próprios, que são geridos e manutenidos pelo próprio pessoal de informática da Unidade. Ao se utilizar dispositivos externos, isso acarreta em uma grave falha de segurança, uma vez que esses dispositivos podem ter sido contaminados por outras redes e não há um controle de segurança sobre as permissões de uso, aplicativos e sobre aexistência e regras do antivírus. A ESET, empresa de segurança da informação, expõe em artigo de 2012 que, embora a utilização de laptops pessoais na empresa aumente a produtividade e reduz custos para a empresa, por outro lado, cria novos riscos à segurança da informação, como a exposição da rede corporativa a malwares, o roubo ou extravio de informações sensíveis, ataques de *phishing* e spam.

No próximo item, foi questionado ao militar se ele tem algum cuidado antes de abrir um e-mail quando está em sua Organização Militar, e, caso a resposta fosse afirmativa, quais seriam os cuidados. Esta pergunta foi formulada tendo em vista que o e-mail é uma das maiores portas de entrada de *malwares* e tentativas de *phishing*. De nossa amostra, observou-se que 93,8% dos militares tomam algum tipo de cuidado antes de abrir um e-mail recebido e, dentre os cuidados assinalados, obtivemos essas respostas:

Grupo / Resposta Obtida	Amostra	
	Valor absoluto	Percentual
Não abro e-mail cuja procedência não conheço	28	87,5%
Abro o e-mail, mas se tem algo estranho fecho logo em seguida.	4	18,8%
Baixo apenas os anexos que sejam imagens/vídeos/documentos de texto	8	25,0%
Verifico se o antivírus está ativo antes de abrir o e-mail	8	25,0%
Mantenho o sistema operacional sempre atualizado. Priorizo o Linux em detrimento do Windows	2	6,3%
Pratico a contra-inteligência. Tudo que desconheço, não	2	6,3%

acesso.		
Nenhum.	2	6,3%

Fonte: O autor

O resultado para esse item foi satisfatório já que demonstrou que grande maioria dos militares toma as precauções básicas ao receber um e-mail. Dos militares que responderam o questionário, 87,5% não abrem e-mail cuja procedência é desconhecida. Além disso, 18,8% abrem os e-mails e, caso observam algo estranho, fecham em seguida. Entretanto observou-se, também, que poucos verificam se o antivírus está ativo antes de abrir um e-mail (25%) e baixam apenas imagens, vídeos ou documentos de texto (25%).

Aliado a questão sobre o e-mail, foi perguntado também sobre a utilização de pendrives pessoais no trabalho, já que esse tipo de mídia removível é, juntamente com o e-mail, um dos maiores vetores de propagação de *malwares*. O resultado foi o seguinte:

GRÁFICO 1– Resposta da amostra sobre a utilização de pendrives pessoais no ambiente de trabalho.

Esse resultado é insatisfatório já que demonstra que a maioria dos militares utilizam suas mídias para transferir arquivos entre computadores do ambiente de trabalho. Como os pendrives pessoais circulam por vários computadores, há uma grande chance de ser infectado por um computador com a segurança debilitada e disseminar esse malware em outros computadores, inclusive os da Unidade.

Outra questão abordada no formulário enviado aos militares diz respeito ao conhecimento dos militares que o sistema operacional Linux, embora seja comprovadamente mais seguro que o sistema operacional Windows, também possui riscos de segurança e pode sofrer ataques pela rede e de malwares. Para isso, foi perguntado se o militar acredita que os vírus afetam apenas o sistema operacional Linux e que os sistemas operacionais Linux (Ubuntu, Debian, entre outros..) não sofrem ação de vírus. O resultado foi o seguinte:

Grupo / Resposta Obtida	Amostra	
	Valor absoluto	Percentual
Não	20	62,5%
Sim	12	37,5%
TOTAL	32	100,0%

Fonte: O autor

Nota-se que a maioria dos militares acreditam que o sistema operacional Linux é imune à ameaças cibernéticas. O grande problema em questão é que, por acreditarem na segurança desse sistema operacional, o militar descuida de outros pontos de segurança, que podem comprometer o dispositivo e a rede interna da OM.

A próxima pergunta questionava se o militar já verificou alguma suposta incidência de vírus nos computadores de sua OM.A resposta obtida foi a seguinte:

Grupo / Resposta Obtida	Amostra	
	Valor absoluto	Percentual
Sim	26	81,3%
Não	6	18,8%
TOTAL	32	100,0%

Fonte: O autor

A grande maioria dos militares (81,3%) afirmaram que já verificaram a incidência de vírus em sua OM. Esse dado corrobora com a necessidade de que O Exército Brasileiro realize gestões a fim de aprimorar a defesa das OM contra ataques cibernéticos e ameaças de *malwares*. Mesmo o dado não sendo preciso, já que outros motivos, além da presença de malwares, possam ter levado ao militar a acreditar que seu computador estava infectado, o valor do resultado obtido, maior que 80%, é preocupante.

Outra pergunta realizada no questionário se refere a existência de aplicativos não autorizados nos computadores dos subordinados. O resultado obtido foi o seguinte:

Grupo / Resposta Obtida	Amostra	
	Valor absoluto	Percentual
Sim, já verifiquei os computadores do subordinado e em pelo menos um existia programas, supostamente baixados pelo usuário, para fins diversos que não sejam relativos ao trabalho.	18	56,3%
Não, Nunca verifiquei os computadores do subordinado.	12	37,5%
Sim, já verifiquei e só existiam aplicativos de uso funcional.	2	6,3%
TOTAL	32	100,0%

Fonte: O autor

A maioria da amostra (56,3%) respondeu que já havia inspecionado os computadores do subordinado e encontrou aplicações não necessárias ao trabalho da Organização Militar e que, supostamente, foi baixada pelo usuário. Outro dado que agrava o dado anteriormente referido é que apenas 6,3% da amostra respondeu que só haviam aplicações funcionais nos computadores. Isso demonstra que as OM não possuem um controle de aplicações instaladas nos computadores funcionais, o que pode comprometer a segurança, uma vez que o militar pode baixar aplicativos maliciosos ou com vulnerabilidades, que seria uma porta de entrada da rede da OM para as ameaças cibernéticas.

A penúltima questão abordada no questionário diz respeito às instruções de Capacitação Técnica e Tática do Efetivo Profissional (CTTEP). Como previsto no Programa Padrão do Exército Brasileiro, as Unidades devem promover, junto ao seu quadro de efetivo profissional, instruções técnicas e táticas a fim de disseminar conhecimentos ao seu público interno sobre diversas áreas. Dessa forma, foi questionado à amostra se eles já haviam tido instrução sobre cuidados a serem adotados a fim de evitar ataques cibernéticos. O resultado obtido foi o seguinte:

Grupo / Resposta Obtida	Amostra	
	Valor absoluto	Percentual
Sim, já houve instrução sobre o tema.	18	56,3%
Não, não houve instrução sobre o tema.	14	43,7%
TOTAL	32	100,0%

Fonte: O autor

Um pouco mais da metadedos militares (56,3%) relataram ter tido instruções sobre cuidados cibernéticos nos últimos três anos. Tendo em vista que, por meio das instruções de CTTEP, os conhecimentos serão transmitidos para todo o efetivo profissional da OM, cresce de importância o estímulo ao aumento dessa atividade que, como consequência direta, elevariam o nível da consciência dos militares sobre os cuidados que devem ser tomados para melhoria da segurança dos meios de TI da Unidade.

A última questão abordada foi a respeito da existência de redes sem fio (*wifi*) na Organização Militar. Redes sem fio são mais suscetíveis a ataques cibernéticos, já que não há necessidade do atacante ter que realizar o contato físico à rede interna da Organização Militar. Além disso, o controle dos dispositivos que se conectam à rede *wifi* é mais complexo e, dessa forma, a tendência é que múltiplos dispositivos se conectem e possam ameaçar a segurança dessa rede. O resultado obtido pela amostra foi o seguinte:

Grupo / Resposta Obtida	Amostra	
	Valor absoluto	Percentual
Não, não há redes sem fio	20	62,5%
Sim, há redes sem fio	12	37,5%
TOTAL	32	100,0%

Fonte: O autor

Dessa forma, verifica-se que há rede *wifi* nas OM da 9ª Brigada Escola, entretanto em poucas OM (37,5%). Como não foi questionado a respeito dos critérios e procedimentos adotados para acesso à essas redes, não tem como se tomar uma conclusão mais aprofundada.

4 CONSIDERAÇÕES FINAIS

Quanto às questões de estudo e objetivos propostos no início deste trabalho, conclui-se que a presente investigação atendeu ao pretendido, ampliando a compreensão sobre o nível de conscientização dos oficiais do Exército quanto aos esforços de prevenção aos ataques cibernéticos atuais.

Diante do expressivo aumento de ataques cibernéticos à empresas e órgãos governamentais, essa pesquisa se torna relevante, uma vez que o Exército Brasileiro pode ser alvo dessa ameaça e sofrer a exposição de informações críticas e dados com classificação sigilosa. Portanto, há necessidade de que se realize gestões de segurança da informação a fim de que medidas sejam tomadas e dificultem o êxito de ataques cibernéticos perpetrados na estrutura de TI do EB.

A revisão de literatura possibilitou concluir que os esforços de prevenção a ataques cibernéticos envolvem um conjunto de ações, entre elas, a conscientização dos militares. Além disso, os recursos humanos são o elo mais fraco na estratégia de segurança cibernética de qualquer organização, porém, quando bem instruídos, se tornam a defesa mais forte.

Com os questionários enviados aos capitães que serviram nos últimos três anos na 9ª Bda Inf Mtz (Es), a fim de verificar o nível de conscientização dos militares sobre a segurança cibernética, pode-se, superficialmente, concluir que a grande maioria entende que suas atitudes também fazem agregam para aumentar a defesa cibernética de uma Organização Militar.

Além disso,a grande maioria tem o conhecimento que o e-mail é um vetor de ataque cibernético e toma os cuidados necessários para não ser contaminado ao abrir a caixa de e-mail.Entretanto, a maior parte de nossa amostra diz ter utilizado o seu notebook e mídias removíveis pessoais no ambiente de trabalho, o que eleva o risco de infecção da rede interna da OM por malwares.

Aliado a esse fato, a maioria dos militares afirmam a existência de aplicações pessoais nos computadores da OM, indicando que não há um controle de aplicações instaladas nos computadores funcionais, o que pode eleva o risco de segurança da OM. Porém, o dado mais alarmante coletado nos questionários é que cerca de 80% dos militares da amostra verificaram a suposta incidência de vírus em computadores de sua OM.

Por fim, verificou-se, que metade dos militares da amostra tiveram alguma

instrução de cuidados cibernéticos nos últimos três anos.

Dessa forma, após identificar o cenário atual do nível de conscientização da amostra, pode-se concluir que existe um certo grau de maturidade na segurança da informação, entretanto carece de recursos humanos mais bem instruidos e políticas internas ativas para regular ações potencialmente perigosas para as atividades cibernéticas.

Recomenda-se, assim, a realização de mais instruções sobre o tema e a aplicação de políticas de segurança da informação mais rígidas, como a proibição da utilização de computadores e mídias removíveis pessoais e o controle das aplicações nos dispositivos funcionais da organização militar.

REFERÊNCIAS

ANBIMA**. MELHORES PRÁTICAS DE SEGURANÇA CIBERNÉTICA.** Disponível em: <https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Seguran%C3%A7a%20Cibern%C3%A9tica%20-%2023_06_2016.pdf/>. Acesso em: 12 nov. 2016

ARTIGO 19**. Brasil: Análise da Estratégia de Cibersegurança .**Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2016/05/Brasil-An%C3%A1lise-da-Estrat%C3%A9gia-de-Ciberseguran%C3%A7a.pdf/>. Acesso em: 12 nov. 2016

BARRETO, Luciano. **Impactos do Ataque Cibernético**. Disponível em: <http://www.cvm.gov.br/noticias/arquivos/2017/20170511-1.html>. Acesso em: 13 mar. 2017

BBVA RESEARCH**. Ataques cibernéticos: una de las mayores amenazas en 2016.** Disponível em: <https://www.bbvaresearch.com/wp-content/uploads/2016/03/Situacion_ED_Mar16_Cap2.pdf/>. Acesso em: 12 nov. 2016

CERT UK. **Common Cyber Attacks: Reducing The Impact**. Disponível em: < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_ Impact.pdf>. Acesso em: 12 nov. 2016

KANAMARU, Márcio.IT4Cio – Internet das Coisas: bilhões de oportunidades para ataques cibernéticos. Disponível em: https://medialinkblog.wordpress.com/2016/11/16/it4cio-internet-das-coisas-bilhoes-de-oportunidades-para-ataques-ciberneticos/>. Acesso em: 12 nov. 2016

PINHEIRO, ALANE COSTA. Guerra Hibrida e Ciberconflitos: Uma Análise das Ferramentas Cibernéticas nos Casos da Síria e Conflito Rússia-Ucrânia. Disponível em: <http://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/XIII_cadn/guerra_hibrida_e_ciberconflitos_uma_analise_das_ferramentas_cibernetica s_nos_casos_da_siria_e_conflito_russia-ucrania/>. Acesso em: 12 nov. 2016

PRICE WATER HOUSE COOPERS. Evolução de ameaças e ataques cibernéticos preocupa empresas. Disponível em: <https://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/cyber-essentials/cyber-essentials-5.pdf>. Acesso em: 14 jun. 2017

REUTERS**. Coreia do Norte intensifica ataques cibernéticos contra o Sul** Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/22634/ Coreia-do-Norte-intensifica-ataques-ciberneticos-contra-o-Sul--diz-Seul/>. Acesso em: 12 nov. 2016

SECURITY REPORT**. Crimes cibernéticos: a nova epidemia digital, global e silenciosa.**Disponível em: <http://securityreport.com.br/destaques/crimes-ciberneticos-nova-epidemia-digital-global-e-silenciosa/>. Acesso em: 12 nov. 2016

WILLIS TOWERS WATSON. **Risco Cibernético**. Disponível em:<http://www.willis.com.br/media/1402/willis-towers-watson_cyber-risk-bulletin_wannacry-ransomware_port_may-2017.pdf> Acesso em: 13 jun. 2017