**ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS**

**CAP COM ANDRÉ KOHLER DAMIÃO**

# GUERRA CIBERNÉTICA: PROTEÇÃO CIBERNÉTICA

MONITORAMENTO DE REDES E SISTEMAS E LEVANTAMENTOS DE VULNERABILIDADES

**Rio de Janeiro**
**2018**

**ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS**

**CAP COM ANDRÉ KOHLER DAMIAO**

# GUERRA CIBERNÉTICA: PROTEÇÃO CIBERNÉTICA
MONITORAMENTO DE REDES E SISTEMAS E LEVANTAMENTOS DE VULNERABILIDADES

Trabalho acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Gestão Operacional.

**Rio de Janeiro**
**2018**

**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 Com ANDRÉ KOHLER DAMIÃO**

Título: **GUERRA CIBERNÉTICA: PROTEÇÃO CIBERNÉTICA**
MONITORAMENTO DE REDES E SISTEMAS E
LEVANTAMENTOS DE VULNERABILIDADES

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

*APROVADO EM* _____/_____/_____ *CONCEITO:* _____

**BANCA EXAMINADORA**

| Membro | Menção Atribuída |
|---|---|
| _____<br>**-**<br>Cmt Curso e Presidente da Comissão | |
| _____<br>**- Cap**<br>1º Membro | |
| _____<br>**- Cap**<br>2º Membro e Orientador | |

_____
**ANDRÉ KOHLER DAMIAO – Cap**
Aluno

# GUERRA CIBERNÉTICA: PROTEÇÃO CIBERNÉTICA
## MONITORAMENTO DE REDES E SISTEMAS E LEVANTAMENTOS DE VULNERABILIDADES

André Kohler Damião
Cézar Flores Malhada Júnior

**RESUMO**

Diante da grande evolução da internet e dos estreitamentos das relações diplomáticas e comerciais no mundo virtual, este trabalho visou abordar as principais ameaças digitais que existem no ciberespaço, as vulnerabilidades das redes, hardwares e softwares das Organizações Militares do Exército Brasileiro e os danos que possíveis ataques podem ocasionar. Sua finalidade principal é conscientizar os militares sobre a real ameaça de ataques cibernéticos, propondo que haja maior preocupação com os procedimentos de segurança lógica ou física e a necessidade da atualização constante dos mesmos. Para atingir os objetivos, esse artigo científico foi desenvolvido através de uma pesquisa bibliográfica, sendo comparada e fundamentada através de entrevistas e discussão no grupo focal com militares que possuem experiência pessoal na área cibernética. Apresenta conceitos sobre os principais *malwares* e métodos que os *hackers* usam nos ataques e elenca quais desses são mais prováveis contra nossos sistemas. São abordados quais são as vulnerabilidades dos nossos equipamentos e redes, diante das prováveis ameaças discorridas. A preocupação com a segurança cibernética reside na proteção da imensa quantidade de dados sensíveis, pessoais e institucionais, que possuem nossos bancos de dados. Na conclusão, as informações colhidas ao longo do trabalho são cruzadas e comparadas, enfatizando-se o uso dos procedimentos de segurança digital corretamente por todos usuários, como forma de proteção cibernética contra cibe ataques.

**Palavras-chave:** Ameaças. *Malwares*. Vulnerabilidades. Proteção cibernética. Dados sensíveis. Ciberespaço.

**ABSTRACT**

Against of the great increase of the internet and the narrowing of diplomatic and commercial relationships in the virtual world, this work has aimed to approuch the digital threats that exist in cyberspace, the vulnerabilities of the network, hardwares and softwares of the Military Organizations of the Brazilian Army and the damage that attacks could bring on. Its main goal is to make the military a major concern of the real threat of cyber attacks, to have a greater preoccupation on security procedures and its continuous update. To reach this objective, this study was developed through a bibliographic research, was compared and substantiated itself through interviewes and a focus group argument with militaries with na experience at the cybernetic area. Presente the mean of major malwares and hackers attack methods and point out the most likely that could to be against our systems. The vulnerables of our systems and networks are approaches in face od the probable threats that have been discussed. The cybernetics security concern resides in the protection of the big sensitive data, the people and the institutions data that own our databases. In conclusion, the informations collected throughout the work are crossed and compared, with emphasis on the right use of digital security procedures by all users, as a form of cybernetic protection against cyber attacks.

**Keywords:** Threats. Malwares. Vulnerabilities. Cybernetic protection. Sensitive data. Ciberespace.

# 1 INTRODUÇÃO

O progresso dos meios digitais no ciberespaço é uma constante. A Tecnologia da Informação (TI) evolui conforme novos protocolos e equipamentos surgem, exigindo um contínuo e infindável aprimoramento dos procedimentos de segurança. Diante do avanço tecnológico atual e das crises geopolíticas e sociais, que afetam o mundo moderno, a Guerra Cibernética surge como um meio para afetar as estruturas estratégicas ou táticas de um alvo específico, seja em guerra ou em tempos de paz.

O uso de computadores como meio de hostilidade teve a sua origem utópica nos livros e nas produções cinematográficas da década de 1980. A novela *Neuromancer* que Willian Gibson publicou em 1984, popularizou a palavra *cyber* e um mundo utópico e fictício. Filmes como *Wargames* (JOHNBRADHAM, 1983) e *Sneakers* (PHIL ROBINSON, 1992) expandiram as hipóteses desse uso, ainda em um mundo fabuloso. Porém, em fatos mais tangíveis para época, os filmes *The Net* (IRWIN WINKLER, 1995) e *Hackers* (IAIN SOFTELY, 1995) tiveram um grande impacto cultural. Principalmente quando, aliado a apocalítica previsão de colapso dos sistemas de comunicação da virada do século, o *bug* Y2K (o "*bug* do milênio") assombrou todo o planeta. Assim, criou-se um temor quanto a real capacidade futura do uso do *cyberspace*.

Concomitante, e mesmo anteriormente, com a utopia dos filmes e livros, foi criada, a partir de 1978 até 1993, uma série de normatização de protocolos de segurança eletrônica em tecnologia da informação, a conhecida série *Rainbow Series*. Essas regras, que já previam o perigo iminente, culminaram na criação estadunidense do *Computer Fraud and Abuse Act*, leis que tipificaram os crimes digitais, tendo em 1995 o caso mais midiático: Kevin Mitnick como o primeiro *Hacker* condenado da história.

A cyber Guerra como instrumento de combate foi noticiado pela primeira vez em 2007, na Estônia, quando sites governamentais e de empresas locais tiveram o conteúdo de seus sites modificados. Foram utilizadas técnicas de vandalismo digital conhecido como *defacement* e foram retirados do ar esses endereços eletrônicos, através da técnica *Distributed Denial of Service* (DDoS), que é um ataque de informações em massa até o sobrecarga do sistema alvo. Apesar da invasão ser digital, a Estônia acusou a Rússia de invasão de seu território. Na época a OTAN

reconheceu em público o ataque virtual como uma guerra real, equiparando o ciberataque a um ataque com míssil, unificando assim o mundo digital ao mundo real.

Ocorrido em 2008, na região da Ossétia do Sul, na Geórgia, em um contexto político diferente, já existia uma guerra declarada entre a Rússia e os georgianos. Semelhantemente ao caso da Estônia, houve vários ataques cibernéticos, através das técnicas de *defacement* e DDoS, pela Rússia. O ataque foi mundialmente conhecido como "*cyber*-cerco ao *cyberspace* georgiano". Apesar dos ataques não terem causados danos financeiros ou estruturais, apenas negaram o acesso, do país inimigo, aos seus próprios serviços digitais, a Rússia novamente negou o envolvimento com os ataques.

Quase sempre silencioso, os ataques cibernéticos acontecem com autoria desconhecida, como no Irã, em 2010. Neste caso, tivemos um exemplo de um ataque de um *malware*, programa malicioso, sem o uso da internet. Supostamente criado pela parceria dos Estados Unidos com Israel, o *worm* Stuxnet foi projeto para se propagar através de pen drives contaminados automaticamente e afetar equipamentos eletrônicos que atuassem em determinada frequência programada, não por acaso, era a mesma utilizada por centrífugas a gás de enriquecimento de Urânio.

Os ataques cibernéticos cresceram em importância e em larga escala, em 2014, a *Sony Pictures* teve 100 terabytes de dados roubados. Em 2015, a empresa italiana de vigilância digital *Hacking Team* teve 400 GB de dados propositalmente vazados. Até carros foram crakeados e tiveram as suas funções desabilitadas remotamente. No caso mais famoso, Edward Snowden vazou informações sigilosas de segurança dos Estados Unidos da América denunciando a espionagem digital que esse país realizava contra dezenas de outros países, como por exemplo, o Brasil.

De acordo com o Centro de Estudos de Resposta e Tratamento de Incidentes de Segurança para a Internet Brasileira (CERT.br), os incidentes digitais, que foram reportados, apresentaram um aumento de quase 2000% em duas décadas. Destaque para a evolução dos incidentes de 2013 para 2014, de 352.925 incidentes em 2013, para um total de 1.047.031 incidentes em 2014. Um aumento de 300% em apenas um ano, informações extraídas do Gráfico I abaixo.

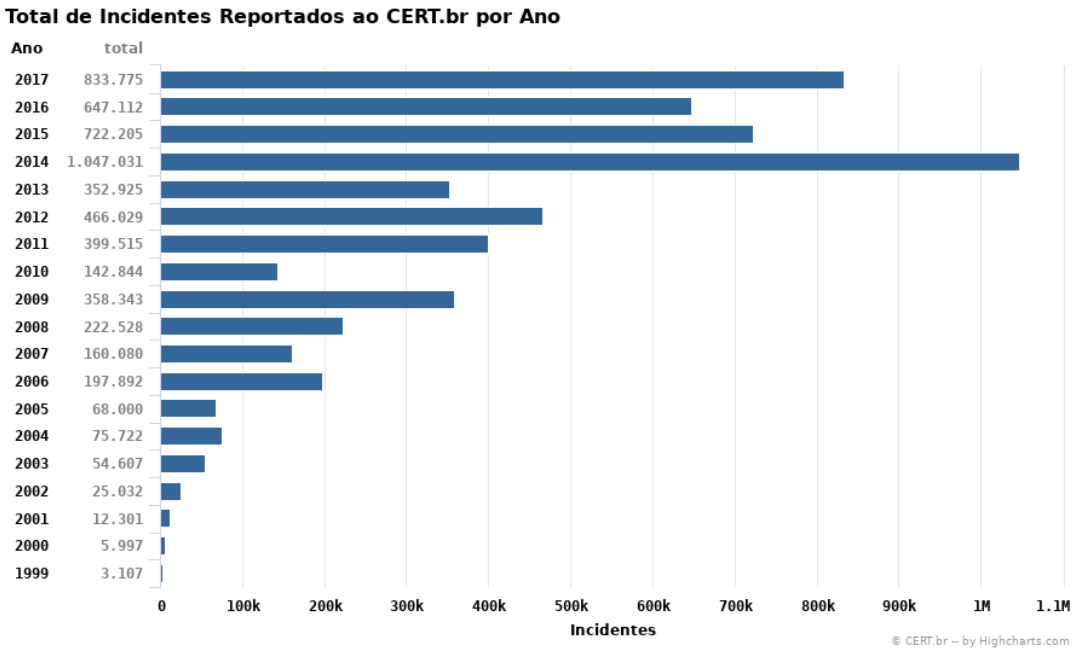


**GRÁFICO 1 -** Estatísticas dos Incidentes Reportados ao CERT.br

Fonte: Cert.Br

No mais atual ataque, em 12 de maio de 2017, uma variação do vírus WannaCry, um *ransoware*, que quando acionado, através de um arquivo enviado automaticamente para milhões de e-mail, ele "sequestra" o computador, criptografando os dados e exigindo um resgate de US$ 300,00 por sistema operacional afetado. Nota-se, portanto, a importância do assunto e a capacidade destrutiva de um simples malware.

## 1.1 PROBLEMA

Atualmente, na Era do Conhecimento, observa-se, por parte das Unidades do Exército Brasileiro e dos militares, a falta de conhecimento ou falta de crença das reais ameaças virtuais que nos circundam. Essa alienação tecnológica, proposital ou não, aumenta as vulnerabilidades e por consequência, o risco de uma possível invasão ou coleta de dados sigilosos.

Quais são as ameaças virtuais que são mais prováveis de serem usadas contra os sistemas das OM? Qual seria o impacto pessoal, financeiro ou para segurança nacional se os computadores das Unidades do Exército sofressem um "sequestro”? Cada OM tem seus procedimentos para segurança da Tecnologia da Informação, qual procedimento é mais eficaz? Quais as maiores vulnerabilidades dos sistemas digitais?

Após a análise e ponderação dos fatos mencionados previamente, foi elaborado o seguinte problema de pesquisa: As Unidades do Exército Brasileiro adotam de forma eficaz os procedimentos mínimos de medidas de proteção cibernética, capazes de diminuir as vulnerabilidades, a um nível aceitável, contra-ataques cibernéticos de malwares em tempo de não-guerra?

## 1.2 OBJETIVOS

A presente pesquisa tem por objetivo geral conscientizar os militares do Exército Brasileiro sobre a importância de procedimentos mínimos de segurança, lógicos e físicos, que diminuam, a um nível aceitável, as vulnerabilidades contra-ataques cibernéticas de malwares em tempo de não-guerra.

Para viabilizar a consecução do objetivo geral de estudo e de facilitar o entendimento desta pesquisa, foram elencados alguns objetivos específicos, abaixo relacionados, que permitiram o encadeamento lógico do raciocínio descritivo apresentado neste estudo:

a) Analisar os principais malwares utilizados na internet, suas variações e finalidades;

b) Identificar as principais formas e modelos utilizados nos ataques cibernéticos em instituições do Brasil e do mundo;

c) Identificar os principais e mais eficazes procedimentos de segurança, em instituições do Brasil e do mundo, existentes para proteção contra-ataques cibernéticos;

d) Identificar as medidas que as Unidades do Exército Brasileiro executam para diminuição das vulnerabilidades contra malwares e *hackers*; e

e) Analisar a aplicação dos Comandantes, dos gerentes de TI e dos usuários das Unidades do EB.

## 1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

A presente pesquisa busca a conscientização do Exército Brasileiro para a crescente onda de ataques cibernéticos. Como dito em entrevista ao estadão pelo Coronel Luís Cláudio Gomes Gonçalves, coordenador da implantação do Centro de Defesa Cibernética do Exército, que exemplifica a importância do assunto "O mundo mudou, e hoje uma equipe de dez pessoas mal-intencionadas, com grande

conhecimento, pode fazer estragos enormes em estruturas sofisticadas" (LUPION, 2011).

Diante das ameaças reais e o perigo que elas representam, o assunto requer uma profunda análise, acompanhada de ações efetivas, para proteção dos interesses, dados profissionais e pessoais das Organizações Militares do Exército Brasileiro.

Diariamente os computadores das diversas Unidades do Exército Brasileiro são afetados por malwares de baixo risco, causando pequenas avarias ou simples incômodos. Mas qual seria o impacto que causaria se, por exemplo, todos os computadores das OM sofressem ataque do vírus tipo Wannacry e tivessem seus dados sequestrados.

Nesse sentido, o presente estudo se justifica por promover uma pesquisa a respeito da real capacidade das Unidades do EB, e do conhecimento acerca do assunto dos militares de TI e militares da administração, do qual se espera, com a conscientização, diminuir as vulnerabilidades de rede.

## 2 DESENVOLVIMENTO

Diante do problema exposto, para colher subsídios úteis para conscientizar os militares acerca dos procedimentos lógicos e físicos de segurança digital, esta seção irá levantar as principais formas de ataques a Redes e Sistemas e alguns dos procedimentos mínimos necessários para diminuição das vulnerabilidades em uma OM do Exército Brasileiro. Desta forma, pretende-se criar uma conscientização das reais ameaças virtuais e os possíveis danos a dados sigilosos pessoais e institucionais.

Os métodos elencados nesta seção visam, inicialmente quanto a forma de abordagem do problema, levantar, através de pesquisa bibliográfica, as formas de ciberataque e ameaças existentes no ciberespaço que possam afetar as Unidades do EB.

Quanto ao objetivo geral, será empregada uma pesquisa descritiva, através de entrevista e discussão no grupo focal, para entender se existem e quais são os procedimentos para diminuir as vulnerabilidades das Redes e Sistemas das Unidades do EB. Caso positivo, verificar se esses métodos são eficazes.

Posteriormente, fruto da avaliação dessas estratégias, comparar-se-á com outras medidas de proteção adotadas em outros Exércitos e instituições.

## 2.1 REVISÃO DE LITERATURA

O delineamento da pesquisa foi iniciado a partir dos primeiros relatos de uso do ataque cibernético, a fim de buscar uma solução para o problema de pesquisa, estando baseada em uma revisão de literatura nos limites de jan/1978 a jan/2018. Essa definição temporal se firmou na necessidade dos conhecimentos técnicos sobre o assunto, diante da constante evolução das formas de ataque cibernético e a verdadeira preocupação com o assunto se iniciou nos últimos anos.

O limite anterior foi determinado buscando contemplar as primeiras normatizações sobre o assunto, os protocolos de segurança eletrônica *Rainbow Series*, base para a tipificação dos crimes digitais nos Estados Unidos, *Computer Fraud and Abuse Act*.

Foram utilizadas as palavras-chave ameaças, *malwares*, vulnerabilidades, proteção cibernética, dados sensíveis e ciberespaço, juntamente com seus correlatos em inglês e espanhol, em sítios eletrônicos de procura na internet e biblioteca de monografias da Escola de Aperfeiçoamento de Oficiais (EsAO), sendo selecionados apenas os artigos em português, inglês e espanhol.

a. Critério de inclusão:

- Estudos publicados em português, espanhol ou inglês, relacionados à ciberataque, ciberterrorismo, análise de redes e Defesa Cibernética;

- Livros, estudos, matérias jornalísticas e doutrinas existentes que retratam as formas de ataque cibernético, vulnerabilidades de rede e formas de defesa; e

- Estudos qualitativos sobre os procedimentos eficazes para proteção cibernética.

b. Critério de exclusão:

- Estudos que possuem como foco a defesa cibernética estritamente em guerra ou operações; e

- Estudos com foco específico e detalhado nos malware.

## 2.2 COLETA DE DADOS

Na sequência do aprofundamento teórico a respeito do assunto, o delineamento da pesquisa contemplou a coleta de dados pelos seguintes meios: entrevista exploratória e grupo focal.

### 2.2.1 Entrevistas

Buscando a ampliação do conhecimento teórico do assunto e de identificação das experiências em ciberespaço, foram realizadas entrevistas exploratórias com os seguintes especialistas, em ordem cronológica de execução:

| Nome | Justificativa |
|---|---|
| PEDRO HENRIQUE DE OLIVEIRA SOUZA – Cap EB | Curso de Guerra Cibernética<br>Analista de Inteligência em Cibernética (CDCIBER) |
| FELIPE RODRIGUES DE VASCONCELLOS – Cap EB | Instrutor do Curso de Guerra Cibernética |

**QUADRO 1** – Quadro de Especialistas entrevistados
Fonte: O autor

### 2.2.2 Grupo Focal

Devido à natureza especializada do assunto e para finalizar a coleta de dados, foi gerenciado um grupo focal, para debater os resultados coletados nos questionários, com os seguintes especialistas:

| Nome | Justificativa |
|---|---|
| ASAEL DA SILVA VAZ – Cap EB | Curso de Guerra Cibernética<br>Chefe de Operações do 5º CTA |
| FELIPE RODRIGUES DE VASCONCELLOS – Cap EB | Instrutor do Curso de Guerra Cibernética |
| PEDRO HENRIQUE DE OLIVEIRA SOUZA – Cap EB | Curso de Guerra Cibernética<br>Analista de Inteligência em Cibernética (CDCIBER) |
| LUCAS ROCHA SACRAMENTO – Cap EB | Curso de Guerra Cibernética |

**QUADRO 2** – Quadro de Especialistas participantes do Grupo Focal
Fonte: O autor

Durante a condução do referido grupo, foram comparadas as divergências entre a percepção da amostra, obtida nos questionários, a doutrina do Curso de Defesa Cibernética e as informações coletadas na pesquisa, dentro dos seguintes aspectos:

a) Formas de ataque cibernético;

b) Vulnerabilidades de Rede e Sistemas nas OM do EB;

c) Formas de proteção cibernética.

## 3 RESULTADOS E DISCUSSÃO

O fluxo de dados pela inovação da Internet encurtou as distâncias e trouxe rapidez e oportunidades infinitas, porém, descobriu-se novas formas de delitos e crimes, as ameaças virtuais, por conseguinte, métodos de defesa surgem no intuito de evitar que os usuários tenham seus dados roubados. Esse breve parágrafo resume

a importância deste artigo, pois mostra a causa (malware), o meio (vulnerabilidades) e a consequência (defesa).

As ameaças, são os *hackers,* que se utilizam dos *malwares,* para obter vantagem ilícita dentro do espaço cibernético e roubar informações. Diante do exposto, foi discutido dentro do grupo focal  e do entrevistado os tipos de ataques cibernéticos existentes no ciberespaço, e através de pesquisa, foi levantado as formas e prováveis ciberataques, dentro dos tempos mais recentes, com a Era da Informação e sua sucedânea, a Era do Conhecimento, o ciberespaço se tornou uma inquestionável vantagem num ambiente competitivo e nos contenciosos internacionais, empresariais, militares ou em qualquer ambiente virtual.

Como cita o autor: “especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo.” (LÉVY: 2000), nos ensindando que tudo está interligado.

O Brasil é um dos países mais vulneráveis do mundo quando tratamos de segurança da informação. Possuímos uma produção quase nula em softwares e procedimentos de proteção cibernética originais. Estamos engatinhando em um cibermundo que voa, o desafio é gigantesco, como harmonizar o avanço da tecnologia com a segurança dos dados sensíveis. Precisamos entender nossas capacidades e as ameaças que rodeia nossos sistemas.

Segundo Velandia (2017), as formas de ataque cibernético são *botnets*, negação de serviço (DDoS), *phishing*, ameaça persistente avançada (APT), *man in the middle*, informações retiradas do Ministério do Interior da Alemanha e *Globalsign*, além dessas formas podemos citar os *ransomwares* e *DNS cache poisoning*.

Sobre os *Bots* nos ataques de rede “botnets são basicamente redes de computadores infectados por bots semelhantes. Para quem propaga esse tipo de ameaça, ter centenas de computadores ligados com bots [...] na tentativa de fraudar e enganar os usuários” (FONSECA, 2009).

DDoS são os ataques de negação de serviço, é uma sobrecarga em um servidor, rede ou computador comum para que recursos do sistema fiquem prejudicados para seus usuários. Para isso, o *hacker* utiliza técnicas que enviam diversos pedidos de pacotes para o alvo com o objetivo de que fique sobrecarregado e não consiga mais responder a nenhum pedido de pacote. Impedindo que o usuário

consiga utilizar o sistema, uma das formas mais utilizadas é o uso dos *Botnets*.

*Phishing*, de acordo com o site da Microsoft é um tipo de roubo, que se utiliza de sites ou e-mails fraudulentos, eles são projetados para roubar dados ou informações pessoais, principalmente número de cartão de crédito, senhas, dados de conta ou outras informações. O *phishing* pode gerar uma APT, em que o invasor permanece no alvo infectado sem ser percebido, sem intenção de destruir ou danificar a rede ou computador, apenas esperando para que possa coletar informações valiosas.

*Man in the Middle* é um tipo de prática que o hacker se interpõe entre o alvo e os serviços online dele, colocando várias armadilhas para que o usuário acabe caindo nelas e o hacker colete senhas, logins e códigos de segurança.

O Instituto Internacional Espanhol de Marketing Digital defini o *ransomware* como um software malicioso que infecta o equipamento alvo e codifica o sistema operacional, realizando um “sequestro virtual”. Eles são de difícil detecção, pois se camuflam em links em redes sociais, de atualização, e outras formas de propagação do malware.

*DNS cache poisoning* (*Pharming*) é o rompimento do DNS (Sistema de Nomes de Domínio) em uma rede, mudando a URL (Localizador Uniforme de Recursos) de um site para um servidor diferente, simulando o site original, fazendo com que o hacker possa coletar os dados digitados nesse site, principalmente senhas de banco.

Além desses o *Rootkit*, que é o uso de um *software*, geralmente malicioso, que se camufla em computadores ou servidores, funciona com um *backdoor*, porta de entrada e saída livre ao *Hacker.* Essa ação fará sem a detecção dos mecanismos tradicionais de segurança.

Os Hackers se utilizam dessas e de outras técnicas para diversos fins, conseguir informações, danificar equipamentos ou redes ou financeiro. Independente dessas formas, as OM do Exército Brasileiro precisam se prevenir, para minimizar os danos sofridos de possíveis ataques. O ativista se utiliza da Exploração Cibernética que é a atividade continua de busca de dados úteis nas redes, sistema e equipamentos de seus alvos, para, após um planejamento minucioso, explorando as vulnerabilidades do sistema, provocar o ataque cibernético.

Podemos descobrir a vulnerabilidade digital, com a pergunta – Qual a

fragilidade do sistema? Portanto, a definição de vulnerabilidade é uma fraqueza que deixa livre o atacante para se aproveitar dessa situação. Qualquer brecha, falha, erro ou omissão pode ser enquadrar como vulnerabilidade.

As ameaças citadas anteriormente somente serão efetivas quando encontrada alguma vulnerabilidade na rede ou computador. Cabe ressaltar que não existe, na atualidade, 100% de segurança, ou seja, é impossível pensarmos em não ter vulnerabilidades. Os entrevistados e o grupo focal foram unanimes em citar que as OM possuem muitas vulnerabilidades nos seus meios de TI, e precisam adotar medidas de proteção cibernéticas e reforçar as já existentes, tornando-as efetivas.

Nesta última década, o Exército Brasileiro começou a adotar algumas normas e políticas para proteção própria. Podemos citar 3 (três) formas principais: A Norma para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército (NORTI), do DCT, publicado no Boletim do Exército Nº 34/2008, a Cartilha Emergencial de Segurança de 2011, do DCT e mais recentemente, voltado para Defesa Cibernética em Guerra, o Manual EB70-MC-10.232 – Guerra Cibernética.

Dessas citadas, a mais importante e que orientou este trabalho é a Cartilha Emergencial de Segurança, com diversos procedimentos de segurança de caráter obrigatório para as OM, atualmente, ela baliza as Unidades do Exército na confecção de suas políticas de uso dos meios de TI.

Esse problema não é apenas do Exército Brasileiro, mas de preocupação internacional, se defender das prováveis ameaças e diminuir as vulnerabilidades foi abordado pelo Ex Ministro da Defesa, Celso Amorim, em sua palestra sobre Estratégia Nacional de Defesa (END), destacada parte de suas falas:

> "Em geral, nas últimas décadas, fomos poupados de grandes conflitos de escala global, mas nunca podemos ter certeza de que eles não voltarão a ocorrer. Mesmo que não sejam catastróficos, como se pensava na Guerra Fria, pode haver outro tipo de conflito. E temos que cuidar dos nossos recursos, dos nossos interesses". (AMORIM, 2012)

A END evidenciou a preocupação com a área cibernética no nível de segurança nacional. Como consequência direta para o EB, em meados de 2012 foi criado o Centro de Defesa Cibernética (CDCiber), atualmente com curso anual para preparação e formação de militares na área.

No mundo lógico e físico existe diversas formas de proteção cibernética, o grupo focal definiu como as principais formas e procedimentos, mais eficazes, ao alcance dos gerentes de TI, as seguintes maneiras: monitoramento e segurança da

borda (firewall), politica de uso de meios de TI, análise de login, conscientização dos usuários, segmentação de rede e proxy reverso – proteção de servidores.

Como monitoramento e segurança da borda também denominado "monitoramento de informações de segurança (SIM)" ou "monitoramento de eventos de segurança (SEM)," significa a coleta e a análise de dados, detectando comportamentos suspeitos ou informações de alteração não autorizadas do sistema, utilizando-se de firewalls para protocolos que definirão quais tipos de comportamento da rede devem gerar alertas e a quais tomadas de ação serão utilizadas.

As políticas de uso dos meios de TI estão, na sua maioria, na cartilha emergencial de segurança de TIC que foi distribuída pelo Diretoria de Comunicações e Tecnologia em 2011, de observância obrigatória por todas as Unidades do EB. Essa cartilha estabelece uma série de procedimentos padrões para proteção cibernética contra ameaças cibernéticas, ações lógicas e físicas de usuários e gerentes de TI.

Sobre isso, o mundialmente famoso *hacker Mitnick*, atualmente gerente de segurança, relata a importância da intensa conscientização de todos.

> “O seu risco não diminui com o simples fato de você criar um panfleto sobre a política de segurança ou enviar seus empregados para uma página da intranet que detalha as políticas de segurança. As empresas devem não apenas definir por escrito as regras das políticas, mas também devem se esforçar ao máximo para orientar todos os que trabalham com as informações corporativas ou com os sistemas de computadores para que eles aprendam e sigam as regras” (MITNICK, 2003, p. 202).

Análise de Logs é essencial para o registro de eventos relevantes e monitoramento do comportamento da rede e usuários. Dessa forma, os registros possuem marcação temporal e de autenticidade, podendo durante a análise ser detectado possíveis invasões, as vulnerabilidades, uso indevido e problemas de hardware ou rede.

O papel dos gerentes de TI e do Comandante da OM são fundamentais para a eficácia dos procedimentos de segurança. Não basta apenas a implantação dos procedimentos de segurança, exige uma continua fiscalização e cobrança dos usuários para que todos apliquem corretamente os procedimentos.

A segmentação da rede serve para dividir a rede principal e diversas seções de redes. Dessa forma, o gerente de TI pode alocar maior segurança conforme a

importância dos dados que trafegam nessa rede, impede que todos os computadores da OM sejam afetados por um ataque.

Por último, a utilização de proxy reverso, protege a rede, oferecendo uma camada adicional de segurança, separando ou isolando o servidor original, como cita a autora:

> "O Proxy Reverso, como o próprio nome diz, atua ao contrário do Proxy. Enquanto um Proxy, no modelo convencional, intercepta requisições originadas na rede local (LAN – Local Área Network) com destino à Internet, um Proxy Reverso intercepta requisições originadas na Internet com destino à rede local" (FIDELIS, 2013).

## 4 CONCLUSÃO

Diante do assunto proposto e os objetivos elencados no trabalho, concluiu-se que a presente pesquisa atendeu ao principal objetivo, que é conscientizar os militares sobre a real ameaça virtual, em tempo de paz, e sobre a necessidade de maiores investimentos financeiros e esforços para que sejam criadas medidas atuais e eficazes de proteção cibernética. Essa conscientização é constante e devida por todas os militares, desde o comandante ao soldado recruta. Um delito digital ou erro de procedimento simples pode gerar um dano institucional no limite da projeção da ameaça

A revisão da literatura permitiu delinear o estudo sobre a crescente formas de ataque e ameaças no ciberespaço, a impossibilidade de ter 100% de segurança, ou seja, sem vulnerabilidades, portanto o risco sempre existirá. Estamos dentro de um mundo virtual, impossível a isolação total ou exclusão digital. Assim, cresce de importância a necessidade do monitoramento constante das vulnerabilidades físicas e lógicas, para se prevenir das possíveis ameaças externas.

Dessa forma, entende-se que, apesar de atualmente, existir os procedimentos definidos na cartilha emergencial de 2011, esses são pouco eficazes. Pois, diante da evolução tecnológica assustadora e o aumento da criminalidade virtual, os atuais procedimentos de segurança adotados pelas nossas OM não são totalmente efetivos para proteção dos nossos dados sensíveis, deixando-nos vulneráveis as ameaças.

A compilação das informações adquiridas com a pesquisa e as discussões do grupo focal permitiu elencar que, a ameaça mais comum contra nossos dados sensíveis é a técnica de *Phishing*, o procedimento mais importante para diminuir a vulnerabilidade do sistema é a política dos procedimentos de segurança.

Aliado a esse pensamento, no Brasil os ataques, reportados ao Cert.BR, que mais acontecem são os de *Scan,* que na teoria não é propriamente um ataque, apenas uma varredura do sistema para análise de possíveis alvos. O segundo seria a Fraude, com 90,85% de sites falsos, onde se enquadra o Phishing, conforme gráfico 2 e 3.

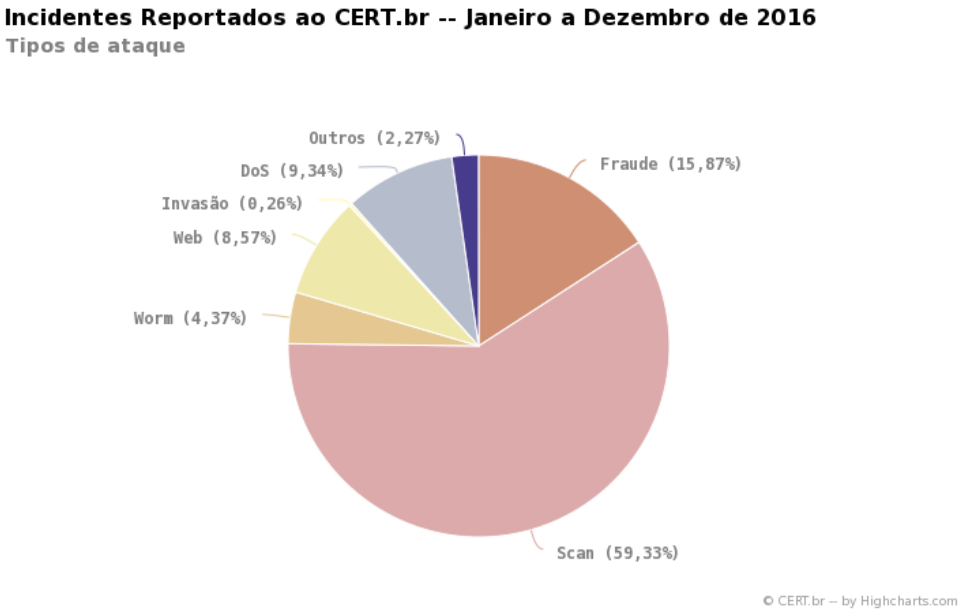


**GRÁFICO 2 -** Incidentes Reportados ao CERT.br - Janeiro a Dezembro de 2016

Fonte: Cert.Br

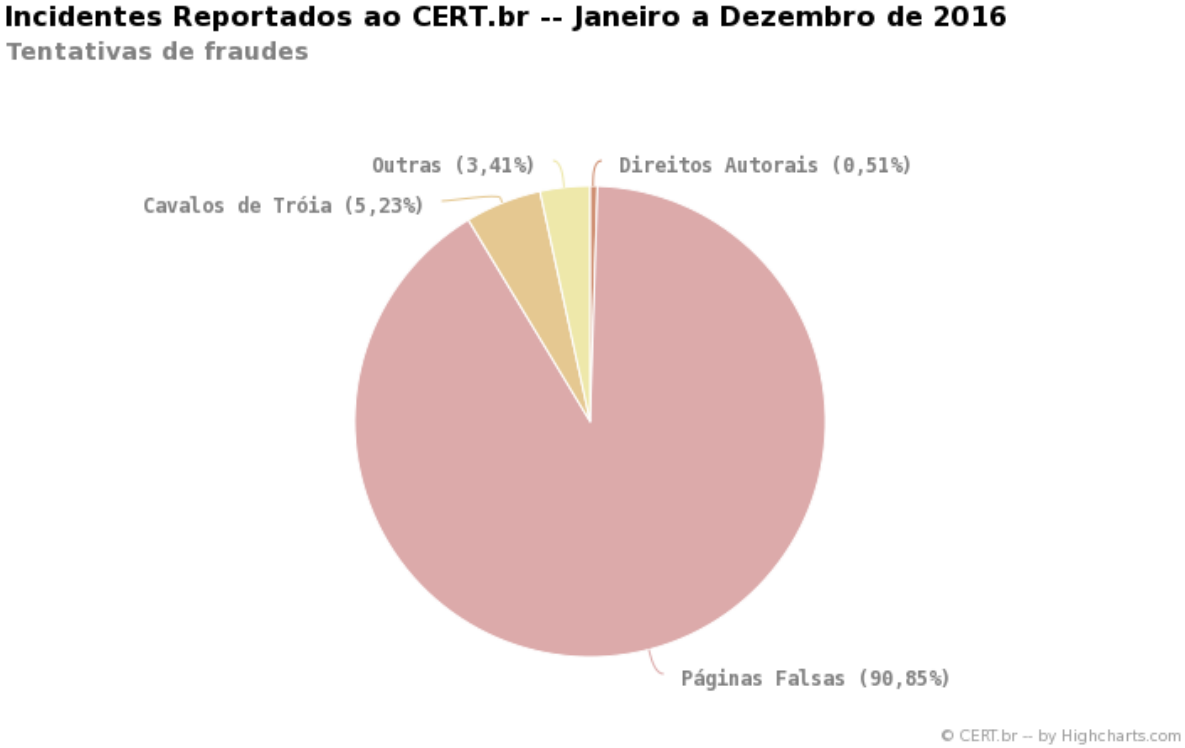


**GRÁFICO 3 -** Incidentes Reportados ao CERT.br - Janeiro a Dezembro de 2016

Fonte: Cert.Br

Um *Phishing* efetivo pode dar ao *Hacker* o acesso a um computador, a rede

interna ou ao banco de dados da OM, podendo assim, causar danos irreparáveis, como o vazamento de dados pessoais e institucionais. O grupo focal sugeriu a criação simulada de Campanha de *Phishing* dentro de cada Unidade. Essa seria feita através da criação de um *Phishing* efetivo, porém inofensivo, através de e-mails (rede da OM) ou SMS (rede privada) enviados a todos os militares da OM, que ao clicarem no e-mail seriam redirecionados para um link forjado que simulasse o site original do conteúdo da mensagem. Essa campanha não geraria dano algum, porém os dados estatísticos retirados desse teste poderiam ser abordados em palestra sobre Defesa Cibernética nas palestras da Capacitação Técnica e Tática do Efetivo Profissional (CTTEP).

Essa palestra é uma das sugestões geradas pelo grupo focal, ministrada pelo Oficial de Contra Inteligência ou pelo gerente de TI, ela serviria para abordar as políticas de segurança da OM, a Cartilha Emergencial, as possíveis ameaças, os erros mais comuns e demais assuntos referentes ao assunto.

No que se refere as demais ameaças, o *Rootkit* pode ser o mais perigoso, pois se o *software* projetado conseguisse entrar em um servidor, ele poderia colher informações, por semanas, sem ser detectado. Assim, o hacker por trás da *backdoor* poderá vasculhar a rede e o banco de dados ligados ao servidor, e obter as informações úteis.

Como prevenção a esse, e a outros malwares, o grupo focal sugeriu duas medidas de proteção. Para verificação do ataque desses softwares, precisa-se de uma análise especializada dos fluxos de informações da rede. Assim, uma das formas de se prevenir seria a realização de cursos específicos na área de segurança de rede para os gerentes de TI, especializando assim o militar que monitora e controla o fluxo da rede.

Outra forma de verificação das vulnerabilidades seria através da simulação "*Pentest*" (teste de intrusão). Projetado para avaliar o nível de segurança antes de um real ataque, o teste visa verificar as vulnerabilidades do sistema, através de um ataque simulado e controlado, o aplicador pode usar técnicas e malwares para capacitar as OM dentro da proteção cibernética.

As políticas de segurança das OM, são delimitadas pela Cartilha Emergencial, mas essa é apenas uma trilha com poucos assuntos e sem detalhes. Dessa forma, cada Unidade estabelece suas próprias políticas, de acordo com as qualificações e experiências do gerente de TI. Todavia, o grupo focal acredita que o ideal seria uma

padronização dessas políticas, feita por um órgão capacitado e de observância obrigatória. Recomenda-se também, a criação de uma renovação anual das informações, para que as políticas consigam acompanhar as medidas de proteção cibernéticas mais atuais.

Também se torna necessário uma maior divulgação, monitoramento e fiscalização das políticas de segurança, para que a ponta da linha, e principal vulnerabilidade do sistema como um todo, realmente entenda a importância dos procedimentos. Essa função é do Comandante da Unidade, definida pela NORTI, no Art. 8º, “Compete ao Comandante, Chefe ou Diretor de OM do Exército realizar pessoalmente, ou delegar, a vistoria dos arquivos hospedados em dispositivos de TI, de propriedade do Exército Brasileiro, e, desde que haja indício substancial de infringência a estas Normas, instaurar a respectiva sindicância” (BRASIL, 2008).

Similarmente, a Cartilha de Segurança, no item 1.3, “Esta Cartilha Emergencial sobre Segurança de TIC, [...] As recomendações contidas nesta publicação são de caráter impositivo, cabendo aos Comandantes, Chefes e Diretores a responsabilidade pelo seu cumprimento” (BRASIL, 2011).

Para auxiliar o Comandante na execução dessas medidas, a Cartilha defini, no item 2.1, que “Cada OM deverá organizar, publicando em Boletim Interno, um Comitê permanente de auditoria interna das medidas de segurança preconizadas na regulamentação vigente” (BRASIL, 2011). Esta comissão é responsável por implementar e fiscalizar, juntamente com o gerente de TI, as medidas de proteção cibernética preconizadas na cartilha e normas internas da OM. Essa será de suma importância para diminuição dos ataques e seus efeitos, pois estaria constantemente procurando as vulnerabilidades existentes no sistema de TI.

Como conclusão, entende-se que a instituição de maior credibilidade do Brasil não pode permitir que dados sensíveis sejam obtidos de seus bancos de dados ilicitamente. Para isso, é de fundamental importância a conscientização constante, por todos os militares, das técnicas e procedimentos de proteção cibernética.

.

## REFERÊNCIAS

BRASIL, Estratégia Nacional de Defesa e Política Nacional de Defesa, p 48-50. 2012;

BRASIL. Exército. **EB70-MC-10.232: Companhia de Fuzileiros**. 1. ed. Brasília, DF, 1973.

BRASIL. Departamento de Ciência e Tecnologia. Boletim do Exércitoº 34, de 22 de agosto de 2008. **Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército;** Brasília, DF, 2008. p. 26.

BRASIL, Livro Branco de Defesa. Disponível em: < https://www.defesa.gov.br/estado-e-defesa/livro-branco-de-defesa-nacional>. Acesso em: 20 mar. 2018

BRASIL, Ministério da Defesa, Diretriz Ministerial 0014 - Integração e Coordenação dos Setores Estratégicos da Defesa. Brasília, 2009.

BRASIL. Núcleo de Informação e Coordenação do Ponto Br. **Cartilha de Segurança para Internet**. Disponível em: <http://cartilha.cert.br/mecanismos/>. Acesso em: 12 jul. 2018.

BRASIL. Núcleo de Informação e Coordenação do Ponto Br. **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponível em: <https://www.cert.br/stats/incidentes//>. Acesso em: 03 ago. 2018.

BRASIL. Tribunal de Contas da União (TCU). **Boas Práticas em Segurança da Informação**. Disponível em: < http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf>. Acesso em: 12 jul. 2018.

CARREIRO, Marcelo. A guerra cibernética: ciberwarfare e a securitização da internet. Revista Cantareira, ed. 17, 2012.

CARVALHO, Paulo Sérgio Melo de. **Setor Cibernético nas Forças Armadas Brasileiras. In: BRASIL. Desafios Estratégicos para a Segurança e Defesa**

**Cibernética**. Brasília, Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

CLARKE, Richard A; KNAKE, Robert K. ***Cyber War: The Next Threat to National Security and What To Do About It***. *New York*: HarperCollins. 2010

DAMIAO, Robson Kohler. **O efeito do setor cibernético sobre uma unidade do Exército Brasileiro e a necessidade de adequação da defesa cibernética.** EsAO, Rio de Janeiro, 2015.

_____.Departamento de Ciência e Tecnologia Site oficial, disponivel em: <http://www.dct.eb.mil.br/>. Acesso em: 22 mai. 2018.

FIDELIS, Donizete. **Proxy Reverso – Uma segurança a mais para seu ambiente.** 2013. Disponível em: < https://www.profissionaisti.com.br/2013/06/proxy-reverso-uma-seguranca-a-mais-para-seu-ambiente/>. Acesso em 07 jul 2018.

FONSECA, Willian. **O que são Bots e Botnets?.** 2009. Disponível em: < https://www.tecmundo.com.br/spyware/2330-o-que-sao-bots-e-botnets-.htm>. Acesso em: 07 jul. 2018

GOLDMAN, Russell. **What We Know and Don't Know About the International Cyberattack.** NY Times, EUA, 2017. Disponível em: <https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html>. Acesso em: 14 jun. 2018.

LEVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

MANDARINO JR, Raphael. **Um estudo sobre a Segurança e a Defesa do Espaço Cibernético Brasileiro.** Universidade de Brasília, Brasília, 2009.

MITNICK, Kevin e SIMON, Willian L. **A arte de enganar.** São Paulo: Editora Pearson Education, 2003.

NETTO, Oscar Rocker. **Ataque cibernético no Brasil cresce 7 vezes mais que média mundial**. Editora Butiá, Curitiba, PR, 2016. Disponível em: <http://riscosegurobrasil.com/materia/ataque-cibernetico-no-brasil-cresce-7- vezes-mais-que-media-mundial.html>. Acesso em: 15 jul. 2018.

_____. Site, <https://iiemd.com/ransomware/que-es-ransomware-que-es-ransomware> Acesso em: 07 jul. 2018

_____. Site, <https://www.microsoft.com/pt-br/security/resources/phishing-whatis.aspx> Acesso em: 07 jul. 2018

STEINBACH, Elvis da Silva. **White hat linux**. Brasil: Editora Alta Brooks, 2017.

VELANDIA, Karenina. **Cinco pontos-chave para se proteger de ataques na internet.** BBC Brasil, São Paulo, 2013. Disponível em: <http://www.bbc.com/portuguese/celular/noticias/2013/11/131101_dicas_proteger_ataque_cibernetico_mm.shtml>. Acesso em: 14 jul. 2018.