Cap QCO Infor JORGE VAGNER VIEIRA DA CRUZ

O FUTURO DA SEGURANÇA CIBERNÉTICA NO BRASIL: PAPÉIS E RESPONSABILIDADES

Trabalho de Conclusão de Curso apresentado à Comissão de Avaliação de Trabalhos Científicos da Divisão de Ensino da Escola de Formação Complementar do Exército, como exigência parcial para a aprovação no Curso de Aperfeiçoamento Militar.

Orientador: Maj QCO LUIZ FERNANDO SOUSA DA FONTE

Salvador
2020

Cap JORGE VAGNER VIEIRA DA CRUZ

O FUTURO DA SEGURANÇA CIBERNÉTICA NO BRASIL: PAPÉIS E RESPONSABILIDADES

Trabalho de Conclusão de Curso apresentado à Comissão de Avaliação de Trabalhos Científicos da Divisão de Ensino da Escola de Formação Complementar do Exército, como exigência parcial para a aprovação no Curso de Aperfeiçoamento Militar.

Aprovado em: ___ / _____ / 2020

LUIZ FERNANDO SOUSA DA FONTE – Maj – 1º Membro
Escola de Formação Complementar do Exército

CARLOS EDUARDO ARRUDA DE SOUZA – Maj – 2º Membro
Escola de Formação Complementar do Exército

ANDERSON BARROS TORRES – Posto – 3º Membro
Escola de Formação Complementar do Exército

O FUTURO DA SEGURANÇA CIBERNÉTICA NO BRASIL: PAPÉIS E RESPONSABILIDADES

Jorge Vagner Vieira da Cruz[1]

Resumo. Os crimes cibernéticos vêm se tornando mais comuns com o passar do tempo, sendo que eles podem afetar de forma negativa as suas vítimas que podem ser pessoas, empresas ou até países. Para combater estes crimes, o Brasil tem desenvolvido leis através de seu legislativo e também se preparado para Guerras Cibernéticas, que já vêm ocorrendo. Neste contexto, este trabalho teve como objetivo apresentar os tipos de ataques cibernéticos, mapear papéis e responsabilidades dos órgãos nacionais que contribuem para fortalecer a segurança cibernética no Brasil e as políticas e as leis brasileiras que vêm sido adotadas neste cenário. Foram apresentadas atribuições do Exército, do legislativo, da polícia e de órgãos da Presidência da República que têm como papel colaborar nas questões de Segurança Cibernética.

Palavras-chave: Segurança Cibernética; Ataque Cibernético; Segurança da Informação

Abstract. Cybercrimes have become more common over time, and they can negatively affect their victims, who can be people, companies or even countries. To combat these crimes, Brazil has developed laws through its legislature and is also preparing for Cyber Wars, which are already taking place. In this context, this work aimed to (i) present the concept and types of cyber attacks and (ii) map the organs and legislation relevant to the issue of Cybersecurity in the Country. The Army, the legislature, the police were assigned and from the Presidency of the Republic's bodies that have the role of collaborating on Cybersecurity issues.

Keywords: Cybersecurity; Cyber Attack; Information security

1 INTRODUÇÃO

O espaço cibernético passou a caracterizar a vida moderna e a maioria das sociedades se digitalizou, inclusive a brasileira. As comunidades digitais também se tornaram um novo fator na política mundial e, portanto, também um novo elemento de poder dentro do equilíbrio da soberania. Além disso, o uso da Internet ainda está se expandindo rapidamente e se tornou o componente principal da conduta cotidiana de todos os atores de nossa sociedade. No entanto, o fácil acesso aos dados traz graves problemas de segurança e ataques cibernéticos a atores públicos e privados são relatados diariamente (JÚNIOR, 2013).

O grande número de ataques tem sérias consequências econômicas e sociais, resultando em oficiais do estado em todos os países reconhecendo a importância de um ciberespaço de segurança. No entanto, o número de ataques cibernéticos está aumentando continuamente e é intrigante que, embora as ameaças cibernéticas sejam enquadradas como um problema de segurança, parece ser difícil implementar medidas eficazes para proteger o ciberespaço (SILVA, 2018).

O ciberespaço (ou espaço cibernético) é considerado como a metáfora que descreve o espaço não físico criado por

[1] Capitão QCO Informática da turma de 2011. Especialista em Aplicações Complementares às Ciências Militares pela EsFCEx em 2011. E-mail: cruz.jorge@eb.mil.br.

redes de computador, notadamente a internet, onde as pessoas podem se comunicar de diferentes maneiras, como mensagens eletrônicas, salas de bate-papo, grupos de discussão, dentre outros. O termo foi criado por Willian Gibson em seu romance “Neuromancer”. (APDSI, 2005).

Nessa pesquisa foi realizado uma busca na base de dados *Scopus* foi realizada no dia 08/07/2020, com os termos de busca “segurança”, cibernética* e brasil* nos campos título, abstract e palavras-chave, sem limitação de data das publicações. O uso do * serve para ampliar a quantidade de artigos recuperados com as variações dos termos segurança e segurança ou brasil.

É importante que sejam feitos estudos que esclareçam o cenário atual a respeito da segurança cibernética no Brasil e no mundo.

2 PROBLEMA DE PESQUISA

A principal indagação contida nesta pesquisa é a de encontrar argumentos para compreender o seguinte questionamento: Como os órgãos nacionais estão lidando com a segurança cibernética e as proteções das infraestruturas?

3 OBJETIVO

3.1 Objetivo Geral

Neste contexto, este trabalho tem como objetivo apresentar um estudo sobre segurança cibernética no Brasil, com ênfase nas Forças Armadas direcionado ao Exército Brasileiro.

3.2 Objetivos Específicos

Com a finalidade de delimitar e alcançar o desfecho esperado para o objetivo geral, levantou-se objetivos específicos que irão conduzir na consecução do objetivo deste estudo, os quais são transcritos abaixo:

a) Definir segurança cibernética.
b) Descrever os tipos de ataques cibernéticos.
c) Identificar os papéis e responsabilidades dos órgãos nacionais.
d) Analisar a Segurança cibernética no Brasil.
e) Elencar as políticas e as leis brasileiras que vêm sido adotadas neste cenário.

4 JUSTIFICATIVA

A presente pesquisa justifica-se pela necessidade de desenvolver um trabalho investigativo de nível acadêmico acerca da abrangência do tema, a fim de compreender conceitos e práticas sobre Segurança Cibernética no Brasil, dentro do contexto militar, relacionando-o às responsabilidades da Força alicerçadas pelo Plano de Estratégia Nacional de Defesa.

O que impulsionou a realização deste trabalho foi o entendimento de que a Segurança Cibernética no Brasil é um assunto atual, que em função de dispositivos legais tornou-se atribuição do Exército Brasileiro e, portanto, direta ou indiretamente deve ser de conhecimento de todos os integrantes da Força Terrestre.

Assim como a Segurança da Informação não é responsabilidade exclusiva dos profissionais de Tecnologia da Informação de uma corporação, entender o conceito de Segurança Cibernética e como ela se insere no contexto de uma intervenção militar também é fundamental.

5 METODOLOGIA

A realização do trabalho contou com a utilização da metodologia de Análises Bibliométricas. De acordo com KITCHENHAM et al. (2009), a Revisão Sistemática é realizada a partir de propostas e questões de pesquisas, das quais são realizadas um levantamento bibliográfico para obter dados conforme os

questionamentos. Ao realizar o levantamento bibliográfico, seu processo é guiado por fatores de exclusão e inclusão, orientam a leitura dos artigos por critérios estabelecidos no início da pesquisa. O protocolo de pesquisa é o conjunto formado pelas questões e critérios de exclusão e inclusão.

A aplicação de técnicas Bibliométricas, consiste na utilização de ferramentas de *software* (*VOSviewer*, *Gephi* etc) que permitem o mapeamento, a organização, o tratamento e a análise sistematizada dos dados de trabalhos científicos, oriundos da base *Scopus*, com o objetivo de extrair informações e gerar conhecimento acadêmico.

6 SEGURANÇA CIBERNÉTICA

A segurança cibernética é a prática de defender computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e dados armazenados nestes sistemas. Também é conhecido como segurança da tecnologia da informação ou segurança da informação eletrônica. O termo se aplica a vários contextos, da empresa à computação móvel, e pode ser dividido em algumas categorias comuns (JÚNIOR, 2013).

As atividades relacionadas a defesa de computadores, dispositivos móveis e sistemas eletrônicos em geral são chamadas "Segurança Cibernética". Esta disciplina é frequentemente chamada de "segurança da tecnologia da informação" ou "segurança da informação eletrônica". O termo é uma generalização e pode aplicar a computadores de mesas presentes na casa ou no escritório de seus usuários ou a dispositivos embarcados diversos (SILVA, 2018).

Abaixo são apresentados alguns contextos a que este termo pode ser aplicado.

Segurança de rede: proteção de uma rede contra atacantes ou *malware* invasores (NAKAMURA; GEUS, 2002).

Segurança do aplicativo: mecanismos implementados no *software*. A preocupação com a segurança deve se iniciar no estágio de projeto do *software* e ser codificado na fase de implementação (SILVA, 2018).

Segurança da informação: refere-se a integridade e a privacidade das informações armazenadas ou sendo transferidas entre os dispositivos eletrônicos (NETO; SILVEIRA, 2007).

Segurança operacional: processos e iniciativas operacionais que visam a manipulação de ativos de dados de forma segura. As empresas devem determinar políticas que visam o armazenamento e o compartilhamento correto de informações (ESCUDEIRO, 2015).

Recuperação de desastres / Continuidade dos negócios: são as políticas que determinam como a organização reage a incidentes de segurança cibernética ou a falhas que podem levar a alguma perda de dados (GUINDANI, 2008).

Educação do usuário final: ensinar os usuários a manipular de forma adequada os sistemas de educação é fundamental. Caso o usuário não esteja educado, os sistemas de proteção são inúteis. Por exemplo, não adianta o investimento em *Firewalls* se os usuários inserem *pendrives* nos computadores infestados de vírus (ALVES, 2010).

7 A ESCALA DA AMEAÇA CIBERNÉTICA

A ameaça cibernética no mundo aumenta aceleradamente, existindo uma quantidade crescente de violações de dados todos os anos. Um relatório da *RiskBased Security* revelou que chocantes 7,9 bilhões

de registros foram expostos por violações de dados apenas nos primeiros nove meses de 2019. Esse número é mais que o dobro (112%) do número de registros expostos no mesmo período em 2018 (HELP NET SECURITY, 2019).

Serviços médicos, varejistas e entidades públicas foram as que mais sofreram violações, com criminosos maliciosos responsáveis por grandes partes dos incidentes. Estes setores são atrativos para este tipo de crime devido ao tipo de dados que armazenam, financeiros e médicos, mas todas as empresas que usam redes podem ser direcionadas para dados de clientes, espionagem corporativa ou ataques de clientes (HELP NET SECURITY, 2019).

Com a escala da ameaça cibernética programada para continuar a aumentar, a *International Data Corporation* prevê que os gastos mundiais em soluções de segurança cibernética atingirão maciços *US* $ 133,7 bilhões até 2022. Os governos de todo o mundo responderam à crescente ameaça cibernética com orientações para ajudar as organizações implementam práticas eficazes de segurança cibernética (HELP NET SECURITY, 2019).

Nos EUA, o Instituto Nacional de Padrões e Tecnologia (NIST) implementou uma infraestrutura de segurança ciber. Para combater a proliferação de códigos maliciosos e ajudar na detecção antecipada, recomenda-se o monitoramento permanente dos sistemas eletrônicos (NIST).

A importância do monitoramento do sistema é ecoada nas “10 etapas para a segurança cibernética”, orientação fornecida pelo Centro de Segurança Cibernética do governo do Reino Unido. Na Austrália, o Centro Australiano de Segurança Cibernética (ACSC) publica regularmente orientações sobre como as organizações podem combater as mais recentes ameaças à segurança cibernética (NIST).

No Brasil, o País tem intensificado ações de segurança, principalmente depois de *(i)* ataques cibernéticos terem fraudado o FGTS, em um ataque ao sistema da Caixa econômica e *(ii)* um ataque cibernético ao Banco do Brasil ter furtado mais de R$ 500 mil reais da prefeitura de Iguape, no litoral paulista. As políticas brasileiras serão abordadas nos próximos capítulos (NEGÓCIOS, 2020).

8 TIPOS DE AMEAÇAS CIBERNÉTICAS

As ameaças combatidas pela segurança cibernética são triplas (SYDOW, 2009):

I. O cibercrime inclui atores ou grupos únicos visando a invasão de sistemas computacionais para obter lucro.
II. O ciberataque geralmente envolve a coleta de informações com motivação política.
III. O ciberterrorismo visa minar os sistemas eletrônicos para causar pânico ou medo.

Nas subseções abaixo são apresentados alguns métodos comuns usados para ameaçar a segurança cibernética.

8.1 Malware

Malware é um *software* malicioso. Este tipo de código é um dos perigos cibernéticas mais comuns, o *malware* é um *software* que um cibercriminoso desenvolveu para interromper ou danificar o computador de um usuário legítimo. Frequentemente disseminados por meio de um anexo de *e-mail* não solicitado ou de um *download* legítimo, o objetivo deste tipo de código pode ser *(i)* ganhar dinheiro ou *(ii)* utilização com motivação política (RIEK et al, 2008).

Existem vários tipos diferentes de *malware*, incluindo:

• **Vírus**: um programa de replicação automática que se anexa a arquivos limpos e se espalha por todo o sistema de um computador, infectando arquivos com códigos maliciosos.
• ***Trojans***: um tipo de *malware* que é disfarçado de *software* legítimo.
• ***Spyware***: sistemas que registram as ações do usuário sem o seu conhecimento, para que cibercriminosos possam usar essas informações. Por exemplo, o *spyware* pode capturar detalhes do cartão de crédito.
• ***Ransomware***: *malware* que não permite o uso dos dados que pertencem a um usuário, com a ameaça de apagá-lo, o que permite a cibercriminosos demandarem o pagamento de um resgate.
•***Adware***: *software* de publicidade normalmente utilizado para espalhar *malware* e que se parece com uma propaganda.
• **Botnets**: grupo de sistemas controlados por *malwares*, que os cibercriminosos usam para executar tarefas on-line sem a permissão do usuário.
(cert.br 2020)

8.2 Injeção SQL

Uma injeção de *SQL* (consulta de linguagem estruturada) é um tipo de ataque cibernético usado para controlar e roubar dados de um banco de dados. Os cibercriminosos aproveitam-se de vulnerabilidades no código das aplicações, orientados a dados para inserir código mal intencionado em um banco de dados por meio de uma instrução *SQL* maliciosa. Isso lhes dá acesso às informações confidenciais contidas no banco de dados (UWAGBOLE, 2017).

8.3 Phishing

Phishing é quando os criminosos cibernéticos atacam as vítimas com *e-mails* que parecem pertencer a uma empresa legítima pedindo informações confidenciais. Os ataques de *phishing* geralmente são usados para enganar as pessoas a entregar dados de cartão de crédito e outras informações pessoais (CHIEW; YONG; TAN, 2018).

8.4 Ataque man-in-the-middle

O tipo de ataque chamado *man-in-the-middle* é uma ameaça cibernética em que um cibercriminoso intercepta a comunicação entre dois indivíduos com a intenção de roubar dados. Em uma rede *Wi-Fi* onde há descuido com a segurança, por exemplo, um invasor pode interceptar dados transmitidos do dispositivo da vítima e da rede (CONTI et al., 2016).

8.5 Ataque de negação de serviço

Um ataque de negação de serviço é onde os cibercriminosos impedem que um sistema de computador atenda a solicitações legítimas através do carregamento excessivo de redes e servidores com tráfego. Isso torna o sistema inutilizável, impedindo uma organização de executar funções vitais (WANG et al., 2017).

9 CASOS ENVOLVENDO AMEAÇAS CIBERNÉTICAS

Abaixo são apresentadas algumas das ameaças cibernéticas mais recentes relatadas pelos governos do Reino Unido, EUA e Austrália.

9.1 Caso do Malwares Dridex

Em dezembro de 2019, o Departamento de Justiça dos EUA (DoJ) acusou o líder de um grupo de criminosos cibernéticos organizado por sua parte em um ataque global de *malware Dridex*. Essa campanha maliciosa afetou o público, governo, infraestrutura e negócios em todo o mundo (CISO, 2019).

Dridex é o nome de um cavalo de Troia que ataca sistemas financeiros e possui diversos recursos. Criado no ano de 2014, ele atua através de *e-mails* de *phishing* ou *malware* existente. Capaz de roubar senhas, detalhes bancários e informações privadas que podem ser usados em transações fraudulentas, causou enormes perdas financeiras de uma grandeza que chega às centenas de milhões de dólares (CISO, 2019).

9.2 Golpes de Engenharia Social

O FBI (polícia federal norte americana) no mês de fevereiro deste ano, alertou os cidadãos dos EUA para estarem cientes das fraudes de confiança que os cibercriminosos cometem usando sites de namoro, salas de bate-papo e aplicativos. Os criminosos aproveitam as pessoas que procuram novos parceiros, enganando as vítimas e dando dados pessoais (WINDER, 2020).

9.3 Malware Emotet

No final de 2019, o *Australian Cyber Security* Center alertou as organizações nacionais sobre uma ameaça cibernética global generalizada do *malware Emotet* (WINDER, 2020).

10 POLÍTICAS E ORGANIZAÇÕES VOLTADAS A CIBER SEGURANÇA NO BRASIL

O trabalho de (EDSON, 2019) fez um levantamento sobre a responsabilidade do Exército Brasileiro no combate a ataques cibernéticos ao país e, como já foi abordado acima, o governo vem adotando medidas contra-ataques cibernéticos, que vêm se tornado mais comuns (NEGÓCIOS, 2020). Neste capítulo estes pontos serão explorados em mais detalhes.

O Exército Brasileiro é o responsável pela segurança nacional neste caso, conforme definido pelo artigo 142 da constituição (PLANALTO)

> As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas, com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República, e destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem.

O Exército deve atuar conforme definido pela legislação internacional, definida pelo DICA (Direito Internacional de Conflitos Armados). Esta legislação aponta que mecanismos de ataque e defesa de guerra cibernética não devem atingir a população civil (EDSON, 2019). No Brasil, a Estratégia Nacional de Defesa delegou ao Exército Brasileiro o espaço cibernético nacional (EDSON, 2019).

O Exército Brasileiro atua dividido em três setores na atualidade: o cibernético, o espacial e o nuclear. O setor cibernético tem como objetivo visualizar o espaço brasileiro integralmente sem a dependência de sistemas ou tecnologia estrangeira. Adicionalmente, é de responsabilidade do setor cibernético, desenvolver sistemas eletrônicos capazes de integrar as três forças - exército, marinha e aeronáutica (EDSON, 2019).

Antes da Copa do Mundo de 2014 e das Olimpíadas de 2016 foi criado o Centro de Defesa Cibernética (CDCiber),

vinculado ao Ministério da Defesa, o qual tem como objetivo a atuação mais ostensiva no campo da guerra cibernética. Exemplo de atuação do CDCiber foi a parceria firmada com o SERPRO (Serviço Federal de Processamento de Dados), que visa o intercâmbio de informações a respeito de Defesa Cibernética e processamento de dados (EDSON, 2019).

A guerra cibernética é formada por políticas adotadas para ataques ao Estado, contudo os cidadãos também podem sofrer ataques cibernéticos. Estes podem ser efetuados contra cidadãos e indivíduos. Para isso, um conjunto de leis foram criadas. Conforme constatado por (PEDROZO, 2019), as leis possuem punições brandas, sendo que no país existem três leis a respeito de ataques cibernéticos: *(i)* Lei Carolina Dieckmann *(ii)* Marco Civil da Internet e a *(iii)* Lei Geral de Proteção de Dados.

A Lei Carolina Dieckmann, cujo nome se refere a atriz que teve algumas de suas fotos roubadas e distribuídas na internet (PEDROZO, 2019). Esta lei consistiu em uma alteração no artigo 154 do código penal para tipificar crimes que consistem em *"invadir, adulterar ou destruir dados ou informações sem autorização"(*PLANALTO). O texto impõe condições para qualificar o crime, cuja pena máxima, com todos os agravantes é no máximo 3 anos. Punição considerada baixa por PEDROZO (2019).

Ainda de acordo com o mesmo autor, o Marco Civil da *Internet* "prevê proteção da privacidade, proteção dos dados pessoais, inviolabilidade da intimidade e da vida privada, entre outros pontos da vida on-line regulamentados". Nele privacidade e segurança são mutualmente dependentes e não há o fortalecimento de questões referentes ao *copyright*, que eram esperadas e deverão ser apresentadas em outras leis (ARNAUDO, 2017).

A LGPD contém ao todo sessenta e cinco artigos, sendo o primeiro responsável por trazer o objetivo geral da lei, que segue abaixo (BRASIL, 2018).

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A lei 12.735/12 determinou a criação de delegacias especializadas em crimes cibernéticos. Muitos estados já vêm seguido a lei e implementaram as referidas delegacias (MOLITOR, 2017) por parte dos governos estaduais.

É importante destacar também o papel do Gabinete de Segurança Institucional da Presidência da República, que possui a tarefa de zelar pela Segurança da Informação do Estado. Este possui diversos órgãos a ele subordinados que também desempenham um papel importante na Segurança Cibernética nacional. Estes são apresentados abaixo, juntamente com o seu papel relativo à Segurança da Informação (JUNIOR, 2013).

Comitê Gestor de Segurança da Informação: assessorar a secretaria-executiva do Conselho de Segurança Nacional.
Secretaria de Acompanhamento e Estudos Institucionais (SAEI): acompanhar temas que têm o potencial de causar crises para o Estado.
Agência Brasileira de Inteligência (Abin): Coordena ações do Sistema Brasileiro de Inteligência. A Abin possui o Centro de Pesquisa e Desenvolvimento de Segurança das Comunicações (CEPESC), o qual realiza pesquisa que dizem respeito a segurança das comunicações.
Departamento de Segurança da Informação e Comunicação (DSIC): tem como atribuições planejar, implantar e

coordenar políticas de segurança da informação e comunicações.

Rede Nacional de Segurança da Informação e Criptografia: é uma rede virtual que tem como objetivo a troca de informação a respeito do tema de Segurança da Informação e Criptografia.

11 SEGURANÇA CIBERNÉTICA NO BRASIL

Woloszin apresenta que os ataques cibernéticos e o ciberterrorismo são uma tendência mundial com perspectivas sombrias. E o especialista complementa, que a maior preocupação para o Brasil reside no fato de que os conhecimentos específicos sobre o tema ainda são do domínio de poucos, assim como, os recursos financeiros são insuficientes. (WOLOSZIN, 2009). No entanto, apesar da expansão do uso da Internet nos últimos anos no Brasil, o país ocupa ainda um posicionamento considerado "ruim" em termos do ranking mundial daqueles países mais conectados na Rede, ocupando atualmente o 590. lugar, segundo o World Economic ForumWWF (WWF APUD SILVA, 2009).

A Política de Defesa Nacional (2005), destaca conceitos relevantes para esta pesquisa.

> Segurança é a condição que permite ao País a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais;
>
> Defesa Nacional é o conjunto de medidas e ações do Estado, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas.

Conforme o Manual da Escola Superior de Guerra, Fundamentos da Escola Superior de Guerra (2009, p. 59), "Segurança é a sensação de garantia necessária e indispensável a uma sociedade e a cada um de seus integrantes, contra ameaças de qualquer natureza." A publicação do decreto 3505/2000, que estabeleceu a Política de Segurança da Informação (PSI), a ser implantada pelo GSIPR; no entanto, não houve a definição dos meios a serem utilizados nessa implementação, sendo que, no momento, esta já se encontra defasada perante as mudanças da última década; - criação do Departamento de Segurança da Informação e Comunicação (DSIC) no Gabinete de Segurança Institucional da Presidência da República (GSIPR), em 2006, com o objetivo de coordenar as ações normativas e operacionais no âmbito da Administração Pública Federal (APF), previstas na PSI (HOSANG, 2010)

> A Convenção sobre o Cibercrime, também conhecida como Convenção de Budapeste, é um tratado internacional de direito penal e direito processual penal firmado no âmbito do Conselho da Europa para definir de forma harmônica os crimes praticados por meio da Internet e as formas de persecução. Esta convenção trata basicamente de violações de direito autoral, fraudes relacionadas a computador, pornografia infantil e violações de segurança de redes. (HOSANG, 2010).

Defesa cibernética diz respeito ao conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente (BRASIL, 2011).

> O ambiente virtual não tem fronteiras. Assim, uma rede comprometida pode prejudicar outras, sejam elas públicas, privadas, contíguas ou não. Por isto, a colaboração e a constante interação entre os mais diversos atores são essenciais para garantir um elevado nível de proteção cibernética para todos (MANDARINO JUNIOR, 2010).

Segurança cibernética refere-se à proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da administração pública federal (BRASIL, 2011).

O conceito de segurança faz referência a infraestruturas críticas, as quais são definidas como instalações, serviços, bens e sistemas que, caso sejam interrompidos ou destruídos, provocam sério impacto econômico, político e social à segurança do Estado e da sociedade (Brasil, 2011).

Há ainda o temor de que a modernização tecnológica, especialmente das infraestruturas críticas, possa ser uma porta de entrada para ataques ou sabotagem de possíveis inimigos (CLARKE E KNAKE, 2011). Independentemente da identificação, os fatos mostram que a tendência é que ataques continuarão a ocorrer com frequência e sofisticação ainda maiores (BAUER E VAN EETEN, 2009).

A criação do ComDCiber ocorreu no âmbito do Programa da Defesa Cibernética na Defesa Nacional, do MD, que tem o objetivo de potencializar o setor cibernético no país e do Programa Estratégico Defesa Cibernética do Exército Brasileiro. É importante ressaltar que mesmo antes da criação de qualquer estrutura específica voltada para a Defesa Cibernética, o Exército já possuía a sua Rede Corporativa, a EBNet, de grande importância estratégica e cuja principal finalidade era, e ainda é, proporcionar as bases físicas e lógicas para o funcionamento seguro dos sistemas estratégicos do Exército Brasileiro. A EBNet é um dos principais ativos do Exército Brasileiro a ser protegido no espaço cibernético, tendo em vista a sua importância estratégica como integradora das Regiões 53 Militares (AVELAR, 2018).

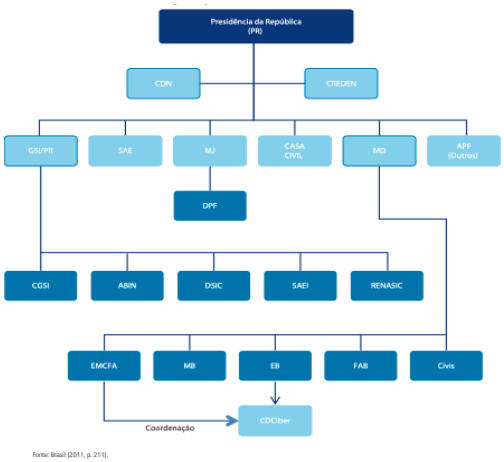
As organizações institucionais Brasileiras:

> A sistematização de instituições e a distribuição de competências entre os organismos para o desenvolvimento de segurança e defesa cibernética é bem recente no Brasil. Algumas instituições que existem há décadas ainda precisam ser adaptadas à nova temática e realidade social. Segurança e defesa cibernética são tratadas no Brasil por diversos organismos. Incluem-se instituições públicas, desde o nível estratégico, de governo, até os operacionais, além da atuação de entidades não governamentais representando o

setor privado (SAMUEL, 2013).

Segurança e defesa cibernética são tratadas, quando necessário, pelo Conselho de Defesa Nacional (CDN). O Art. 91 da Constituição Federal de 1988 define que trata-se de órgão de consulta do presidente da República nos assuntos relacionados à soberania nacional e à defesa do Estado democrático. Constitui um órgão de Estado e tem sua secretaria-executiva exercida pelo ministro-chefe do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). De forma resumida, as ações operacionais em segurança cibernética do governo federal são conduzidas pelo Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional (GSI) da Presidência da República (PR). E a defesa, pelo Centro de Defesa Cibernética (CDCiber), que compõe a estrutura do Exército Brasileiro (EB), vinculado ao Ministério da Defesa (MD). Todavia, existe todo um sistema hierárquico de tomada de decisão estratégica a partir da Presidência da República até que chegue ao nível operacional (SAMUEL, 2013).

Segundo SAMUEL (2013) O Sistema institucional de segurança e defesa cibernética brasileiras.



fonte: Samuel (2013)

(SAMUEL, 2013) No Brasil, fez-se a opção por segregar a direção das ações de segurança da informação e defesa cibernética em dois órgãos distintos e independentes entre si, respectivamente: GSI/PR e CDCiber/EB/MD.

Considerando-se a responsabilidade confiada ao Exército Brasileiro na END, em relação ao desenvolvimento da Defesa Cibernética, era de se esperar que as maiores ações relativas ao tema fossem tomadas no âmbito da Força Terrestre. E realmente, percebe-se nos últimos anos uma série de ações efetivas que demonstram a preocupação com o tema (AVELAR, 2018).

12 FUTURO DA SEGURANÇA CIBERNÉTICA NO BRASIL

O Brasil, nação que passa por um período de grande desenvolvimento social e econômico, precisa atentar e acreditar na possibilidade de ser alvo, em futuro próximo, de ataques cibernéticos, que poderão gerar grandes perdas materiais, quando não catástrofes político-sociais ou humanas (BRASIL, 2011).

A aplicação da lei pode não ser capaz de ajudar diretamente as vítimas de um ataque, mas pode ajudar a proteger outras vítimas potenciais, aumentando o risco de captura, e julgamento dos atacantes, dissuadindo assim ações semelhantes no futuro (BRASIL, 2011).

Equipes especializadas em questões de Segurança da Informação e se projete para um futuro próximo que possuam meios especializados de Defesa Cibernética, a atuação isolada de indivíduos sem o devido conhecimento pode afetar os níveis de proteção a serem alcançados (AVELAR, 2018).

Ferramentas para recrutar e prover *malware* para ser utilizado por *hackers*, podem alcançar um impacto significativo. Esses casos estabeleceram um novo padrão, onde futuros conflitos cibernéticos poderão

ser conduzidos à distância, permitindo aos atores negar a participação nos mesmos ao mesmo tempo em que obtêm benefícios estratégicos ao atingir objetivos políticos (CARNEIRO, 2012).

> No futuro próximo, a guerra de informação iria controlar a forma e o futuro da guerra (CARNEIRO, 2012).

As ações de Defesa Cibernética não são um fim em si mesmas, sendo, geralmente, empregadas para apoiar a condução de outros tipos de operação (CARNEIRO, 2012).

O futuro das capacitações tecnológicas nacionais de defesa depende mais da formação de recursos humanos do que do desenvolvimento de aparato industrial. Daí a primazia da política de formação de especialistas em ciência básica e aplicada (SAMUEL, 2013).

O futuro de um ciberespaço aberto, interoperável, seguro e confiável depende de as nações reconhecerem e protegerem aquilo que deve ser permanente, enquanto confrontam aqueles que trabalham para desestabilizar ou enfraquecer nosso mundo, crescentemente interconectado (SAMUEL, 2013).

Visualiza-se um futuro em que o acesso confiável à internet esteja disponível em qualquer ponto do globo terrestre a um preço que famílias e empresas possam pagar. Computadores se comunicando pelas redes globais e permitindo a comunicação instantânea e confiável entre amigos e colegas. Conteúdo oferecido em linguagem local além de livre trânsito para além das bordas políticas dos países (SAMUEL, 2013).

13 CONCLUSÕES

A quantidade de ataques cibernéticos vem crescendo cada vez mais, sendo que estes ataques podem ter escalas diferentes. Os ataques cibernéticos podem visar atacar um país, indivíduos ou empresas através de diferentes técnicas. Este trabalho apresentou *(i)* o conceito de ataques cibernéticos, *(ii)* as principais técnicas utilizadas nos ataques, *(iii)* alguns casos envolvendo crimes cibernéticos, *(iv)* as legislações e políticas nacionais e internacionais que afetam o combate a ataques cibernéticos no Brasil e *(v)* as responsabilidades de diferentes órgãos do Brasil referente a segurança no espaço cibernético brasileiro.

Diferentes técnicas de ataques cibernéticos foram apresentadas:

i. *Malware*: *softwares* maliciosos
ii. Injeção *SQL*: ataque que controla e rouba um Banco de Dados.
iii. *Pishing*: envio de *e-mail* que parece ser de uma empresa idónea, mas na realidade é um golpe.
iv. Ataque *Man-in-the-midle*: interceptação da comunicação entre dois terminais, com a intenção de roubar informações valiosas.

Depois de apresentar alguns dos principais tipos de ataques, foram apresentados três casos de crimes que envolveram ataques cibernéticos. Dois dos casos apresentados envolveram a utilização de *malwares* famosos e um outro envolveu um golpe que se utilizou de Engenharia Social.

Apresentadas os tipos de ataques e alguns exemplos de ataques relevantes, foram analisadas as legislações internacional e nacional. Foi dada ênfase nos órgãos que visam a aplicação da legislação e a defesa do espaço cibernético.

Este trabalho apontou que o órgão responsável pela defesa do espaço cibernético no contexto da guerra cibernética é o exército brasileiro, o qual segue diretrizes da legislação internacional que tangem o assunto. Além disso, o

legislativo brasileiro possui o papel de criar leis para proteger os cidadãos e empresas, que pune transgressores que praticam crimes cibernéticos. A legislação recente prevê penas para criminosos cibernéticos e também determinou que os estados criem delegacias de crimes que podem ocorrer na internet.

Adicionalmente, foi apresentado o papel do Gabinete de Segurança Institucional da Presidência da República. Foram apresentados as cinco instituições subordinadas a este ministério estatal que possuem papeis definidos com relação a Segurança da Informação do Estado.

Neste contexto, este trabalho teve como objetivo apresentar um estudo sobre segurança cibernética no Brasil, com ênfase nas Forças Armadas direcionado ao Exército Brasileiro. A principal limitação para o desenvolvimento deste artigo foi a dificuldade no acesso a documentos das políticas de segurança cibernética das forças armadas.

Para finalizar, entende que o Brasil, tem diretrizes adotadas e Políticas de Segurança Cibernética de defesa nacional. Sugere-se um aprofundamento maior nas discussões da aplicação dessas políticas de segurança Cibernética em trabalhos futuros.

REFERÊNCIAS

ARNAUDO, Daniel. **O Brasil e o Marco Civil da Internet**. 2017. Disponível em https://www.academia.edu/33142827/O_Brasil_e_o_Marco_Civil_da_Internet_O_Estado_da_Governan%C3%A7a_Digital_Brasileira. Acesso em 06 Jul 2020.

APDSI. Associação para a promoção e desenvolvimento da sociedade da informação. **Glossário da Sociedade da Informação.** Portugal: APDSI. 2005.

ALVES, Cássio Bastos. **Segurança da Informação vs. Engenharia Social : Como se proteger para não ser mais uma vítima / Cássio Bastos Alves**. – Brasília, 2010. 63 f.

AVELAR, José Ricardo Cabral. **A Guerra Cibernética e seus desafios para o Brasil**. Disponível em https://bdex.eb.mil.br/jspui/bitstream/123456789/2893/1/MO%205894%20-%20AVELAR.pdf. Acesso em 06 Jul 2020.

BAUER, J. M.; VAN EETEN, M. J. G. **Cybersecurity: stakeholder incentives, externalities, and policy options**. Telecommunications policy, v. 33, n. 10, p. 706-719, 2009.

BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. **Aprova a Estratégia Nacional de Defesa, e dá outras providências**. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 19 de dezembro de 2008.

BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm Acesso em 08 jul 2020.

CHIEW, Kang Leng; YONG, Kelvin Sheng Chek; TAN, Choon Lin. A survey of phishing attacks: Their types, vectors and technical approaches. **Expert Systems with Applications**, v. 106, p. 1-20, 2018.

CONTI, Mauro; DRAGONI, Nicola; LESYK, Viktor. A survey of man in the middle attacks. **IEEE Communications Surveys & Tutorials**, v. 18, n. 3, p. 2027-2051, 2016.

CISO, advisor. **Trojan Dridex faz ataques em massa a instituições financeiras**. 2019. Disponível em

https://www.cisoadvisor.com.br/trojan-dridex-faz-ataques-em-massa-a-instituicoes-financeiras/ Acessado em 5 jul. 2020.

CARNEIRO, João Marinonio Enke. **A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro** / João Marinonio Enke Carneiro. 2012. 203.

CERT.br. **Estatísticas Mantidas pelo CERT.br**. Disponível em < https://www.cert.br/stats/#:~:text=O%20CERT.br%20mant%C3%A9m%20estat%C3%ADsticas,os%20notificaram%20ao%20CERT.br.> Acessado no dia 06/07/2020.

EDSON, Barbosa de Souza. **A guerra cibernética e o exército brasileiro: uma revisão doutrinária.** Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais. 2019.

ESCUDEIRO, Lopes Diogo Filipe. **O papel das informações no combate ao radicalismo em manifestações violentas de esquerda.** Lisboa, 27 de abril de 2011. Disponível em https://core.ac.uk/download/pdf/322889066.pdf. Acesso em: 15 jul. 2020.

GUINDANI, Alexandre. Gestão da Continuidade dos Negócios. **Revista de Pósgraduação da União Pioneira da Integração Social–Faculdades Integradas (UPIS)**, v. 1, 2008

HELP NET SSECURITY. **5,183 breaches from the first nine months of 2019 exposed 7.9 billion records**. Disponível em: https://www.helpnetsecurity.com/2019/11/14/breaches-2019/. Acesso em: 6 jul. 2020.

HOSANG, Alexandre. **Política Nacional de Segurança Cibernética: uma necessidade para.** CAEP/UnB - Centro De Atendimento E Estudos Psicológicos.

SAMUEL, júnior César Cruz. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Texto para Discussao, 2013.

KITCHENHAM, B. et al. Systematic literature reviews in software engineering - A systematic literature review , **Inf. Softw. Technol**., 2009.

MANDARINO JUNIOR, Raphael. **Segurança e defesa do espaço cibernético brasileiro**, Cubzac Editora, Recife, 2010

MOLITOR, Heloísa Augusta Vieira; VELAZQUEZ, Victor Hugo Tejerina. BREVE PANORAMA SOBRE A LEGISLAÇÃO APLICADA NOS CRIMES ELETRÔNICOS. **Revista de Direito, Governança e Novas Tecnologias**, v. 3, n. 2, p. 81-96, 2017.

NIST. **O elo perdido: integração da segurança cibernética e erm.** Disponível em: https://www.nist.gov/topics/cybersecurity. Acesso em 07 Jul 2020.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. **Segurança de redes**. Berkeley, 2002.

NEGÓCIOS. **Segurança cibernética será reforçada pelo governo**. 2020. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2020/03/epoca-negocios-seguranca-cibernetica-sera-reforcada-pelo-governo.html. Acesso em: 6 jul. 2020.

PLANALTO, **lei nº 12.737, de 30 de novembro de 2012.** Disponível em http://www.planalto.gov.br/ccivil_03/_ato2

011-2014/2012/lei/l12737.htm. Acesso em: 5 jul. 2020.

PEDROZO, Juliano. Lei prevê pena leve para crimes cibernéticos como o do hacker de Moro. **Gazeta do Povo**, São Paulo, v. 1, n. 1, p. 1-1, jun./2019. Disponível em: https://www.gazetadopovo.com.br/republica/crimes-ciberneticos-moro/. Acesso em: 8 jul. 2020.

RIECK, Konrad et al. Learning and classification of malware behavior. In: **International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment**. Springer, Berlin, Heidelberg, 2008. p. 108-125.

SILVA, Washington Rodrigues da. **Análise econômica dos impactos de ataques cibernéticos**. Brasília, 2018. Dissertação (Mestrado - Mestrado em Economia) -- Universidade de Brasília, 2018.

NETO; SILVEIRA, Abner da; SILVEIRA, Marco Antonio Pinheiro da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **JISTEM-Journal of Information Systems and Technology Management**, v. 4, n. 3, p. 375-397, 2007.

SILVA, Luísa Endres Ribeiro da et al. **Desenvolvimento e validação de aplicativo para otimização do posicionamento de eletrodos na técnica de eletroquimioterapia**. Diposnível em http://repositorio.pucrs.br/dspace/handle/10923/12294. Acesso em 6 jul. 2020.

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática**. 2009. Tese de Doutorado. Universidade de São Paulo.

UWAGBOLE, Solomon Ogbomon; BUCHANAN, William J.; FAN, Lu. Applied machine learning predictive analytics to SQL injection attack detection and prevention. In: **2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)**. IEEE, 2017. p. 1087-1090.

WINDER, Davey. **The FBI Issues A Powerful $3.5 Billion Cybercrime Warning. Forbes, USA, fev./2020.** Disponível em: https://www.forbes.com/sites/daveywinder/2020/02/13/the-fbi-issues-a-powerful-35-billion-cybercrime-warning/#430ac5e9187f. Acesso em: 5 jul. 2020.

WANG, Kun et al. Strategic honeypot game model for distributed denial of service attacks in the smart grid. **IEEE Transactions on Smart Grid**, v. 8, n. 5, p. 2474-2482, 2017.