MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DECEX – DESMil – DEPA
ESCOLA DE FORMAÇÃO COMPLEMENTAR DO EXÉRCITO E COLÉGIO MILITAR DE SALVADOR

Cap QCO FÁBIO LUIZ GARCIA

DEFESA CIBERNÉTICA BRASILEIRA: PANORAMA ATUAL E EVOLUÇÃO DAS AMEAÇAS E VULNERABILIDADES EXISTENTES NO CIBERESPAÇO

Salvador
2020

FÁBIO LUIZ GARCIA

DEFESA CIBERNÉTICA BRASILEIRA: PANORAMA ATUAL E EVOLUÇÃO DAS AMEAÇAS E VULNERABILIDADES EXISTENTES NO CIBERESPAÇO

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 obtenção do título de Especialista em Ciências Militares.
Orientador: Major Carlos Eduardo Arruda de Souza.

Salvador
2020

DEFESA CIBERNÉTICA BRASILEIRA: PANORAMA ATUAL E EVOLUÇÃO DAS AMEAÇAS E VULNERABILIDADES EXISTENTES NO CIBERESPAÇO

Fábio Luiz Garcia[1]

Resumo. Nos tempos atuais, o espaço cibernético continua sendo muito explorado por pessoas mal intencionadas, observando-se frequentemente ilegalidades, crimes, terrorismo, dentre várias outras ações, que podem prejudicar e envolver diversos países. Em detrimento dos avanços nacionais, observados nos últimos anos, ainda há dificuldade de se atribuir responsabilidades e reduzir vulnerabilidades. Nesse contexto, através de fundamentação bibliográfica, com abordagem qualitativa de caráter exploratório, o estudo tem como objetivo principal analisar algumas das ações desenvolvidas pelo Ministério da Defesa/Exército, após a implementação da Estratégia Nacional de Defesa (2008), no contexto da Defesa Cibernética. Foram elencadas no contexto mundial as principais ocorrências relacionadas a ataques cibernéticos dos últimos anos, bem como as estratégias de defesa que nosso país vem adotando para evitar ocorrências semelhantes. Foram relacionadas algumas ameaças e vulnerabilidades associadas ao meio cibernético e de modo sucinto, possíveis contramedidas corretivas ou de mitigação. Ao longo do trabalho, verificou-se que é de fundamental importância proteger as infraestruturas críticas nacionais, sendo necessária a implementação de meios para a criação de uma estratégia relacionada à segurança das instalações. Ainda há muito a se fazer, mas o conhecimento e a consciência da exponencial evolução das ameaças e vulnerabilidades existentes no ciberespaço, aliado ao constante aperfeiçoamento tecnológico e respaldo jurídico, possibilita o desenvolvimento e a implementação de medidas eficientes na defesa cibernética do Brasil.

Palavras-chave: Defesa Cibernética; Infraestruturas; Ameaças; Vulnerabilidades.

Abstract. Nowadays, cyber space continues to be widely exploited by people with bad intentions, with illegalities, crimes, terrorism, among many other actions, which it may harm and involve several countries. At the expense of national advances, it was observed in recent years that we still have difficulty in assigning responsibilities and reducing vulnerabilities. In this context, through bibliographic basis, with an exploratory qualitative approach, the main objective of the study was to analyze some of the actions developed by the Ministry of Defense / Army, after the implementation of the National Defense Strategy (2008), in the context of Cyber Defense. The main events(occurrences)related to cyber attacks in recent years were listed in the global context, as well as the defense strategies that our country has been adopting to prevent similar occurrences. Some threats and vulnerabilities associated with the cyber environment and in a succinct way, possible corrective or mitigation countermeasures were listed. Throughout the work, it was found that it is of fundamental importance to protect the national critical infrastructures, being necessary the implementation of means for the creation of a strategy related to the security of the installations. There is still much to do, but the knowledge and awareness of the exponential evolution of threats and vulnerabilities in cyberspace, coupled with constant technological improvement and legal support, enables the development and implementation of efficient measures in Brazil's cyber defense.

Keywords: Cyber Defense; Infrastructures; Threats; Vulnerabilities.

[1] Capitão QCO de Informática da turma de 2012. Bacharel em Sistemas de Informação pela Universidade Bandeirante de São Paulo em 2011. Especialista em Aplicações Complementares às Ciências Militares pela Escola de Formação Complementar do Exército em 2012.

1 Introdução

Na chamada era digital, a tecnologia da informação torna-se cada vez mais indispensável na vida das pessoas, oferecendo benefícios, facilidades, soluções e provocando modificações significativas na área social, profissional, econômica e política. Nesse atual processo de globalização da informatização, o valor da informação trafegada no "ciberespaço" e os ativos utilizados tornam-se uma arma estratégica, muitas das vezes imensurável e importantíssima para uma organização.

Esse progressivo e crescente "ciberespaço" ou "*cyberspaço*" trata-se, conforme Rattray (2001), de um ilimitado mundo digital formado por redes globalmente interconectadas, controladas por regras de *software* e protocolos de comunicação, além dos dados que estas redes trafegam. Sobre isso, Mandarino e Canongia (2010, p. 13) afirmam que:

> Todos os dias, milhões de brasileiros acessam a Internet, trocam informações e usam serviços tais como bancários, de comércio eletrônico, serviços públicos federais, estaduais, de ensino e pesquisa, das redes sociais, dentre outros, constituindo uma ampla rede de atividades digitais.

Consequentemente, tem se visto a mudança na maneira de convívio em sociedade, e as pessoas cada vez mais dependentes dessa tecnologia, atraídas pelas facilidades oferecidas pela mesma, como encurtamento de distância e tempo. Devido à característica de interconectividade presente neste ciberespaço, a informação e os ativos que a manipulam estão frequentemente sujeitos à falta de segurança (aspecto muitas vezes preterido, negligenciado ou ignorado) e exposição às ameaças e vulnerabilidades, das quais indivíduos mal-intencionados podem se valer para praticar atividades danosas a esse bem tão precioso.

Segundo CanalTech (2018), atualmente, o número de ataques cibernéticos, das mais diversas modalidades, vem aumentando consideravelmente, causando falhas, indisponibilidades e prejuízos financeiros. Esse número praticamente dobrou no Brasil em 2018, segundo informações do dfndr lab, laboratório especializado em cibersegurança da PSafe. Segundo a pesquisa do 4º Relatório de Segurança Digital no Brasil, feito por aquele laboratório, foram detectados 120,7 milhões de ataques cibernéticos no primeiro semestre de 2018. Este número representa um crescimento de 95,9% (CANALTECH, 2018).

Nesse contexto, Mandarino e Canongia (2010, p. 13) enfatizam a importância da segurança cibernética, mostrando sua função para a manutenção de

estruturas primordiais para uma nação, quando afirmam que:

> A Segurança Cibernética, desafio do século XXI, vem se destacando como função estratégica de Estado, e essencial à manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria informação, dentre outras. Diante de tais desafios, as Nações vêm se preparando, urgentemente, para evitar ou minimizar ataques cibernéticos às redes e sistemas de informação de governo, bem como de todos os demais segmentos da sociedade. Dessa forma, o entendimento sobre a importância da segurança cibernética caracteriza-se cada vez mais como condição *sine qua non* de desenvolvimento, requerendo para tanto, dentre outras ações, a promoção de diálogos e de intercâmbio de ideias, de iniciativas, de dados, e de informações, de melhores práticas, para a cooperação no tema, no país e entre países.

Barros et al. (2011, p. 19), nos traz o seguinte conceito acerca de Defesa Cibernética:

> Conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente. No contexto do preparo e emprego operacional, tais ações caracterizam a Guerra Cibernética.

Por conseguinte, Barros et al. (2011) caracteriza Guerra Cibernética, como o preparo e emprego operacional de técnicas de ataque e defesa cibernética, ou seja, defesa das estruturas críticas e preparação de recursos humanos, de forma a se ter pessoas capacitadas para atuar em uma possível ofensiva ou ataque.

Ao longo do surgimento e evolução do ciberespaço, muitos autores e especialistas do setor, ou ligados a este, fomentavam uma maior tratativa do assunto Segurança/Defesa/Guerra Cibernética, com a visão da necessidade urgente do estabelecimento de fundamentos, normas, doutrinas etc., que abrangessem todos os aspectos ligados ou correlacionados a essas áreas.

Com o estabelecimento do Setor Cibernético, decorrente da aprovação da Estratégia Nacional de Defesa (END), em 2008, a situação evoluiu e dois campos distintos passaram a ser reconhecidos: a Segurança Cibernética, a cargo da Presidência da República (PR), e a Defesa Cibernética, a cargo do Ministério da Defesa, por meio das Forças Armadas (BRASIL, 2008).

A preocupação com o assunto não ficou apenas restrita ao meio militar e tecnológico, com a expansão crescente dos crimes envolvendo a rede mundial de computadores, tivemos nos últimos anos, uma inovação/renovação do assunto no âmbito jurídico. Foram criados importantes mecanismos regulatórios e disciplinadores, como as Leis 12.735 e 12.737, ambas de 30 de novembro de 2012 e a Lei 12.965, de 23 de abril de 2014 (Marco Civil). Tratando-se de importantes mecanismos para a Justiça Brasileira face ao crescente aumento de casos de crimes relacionados com a tecnologia da informação que muitas vezes não eram tipificados.

Tendo em vista as informações apresentadas, vê-se o quanto a temática é

relevante e tem tomado destaque no âmbito governamental, militar, acadêmico e civil, seja nacionalmente ou internacionalmente, e frente a essa justificativa, estaria a nação brasileira preparada ao novo desafio da Defesa Cibernética? A hipótese é de que o Brasil tem o seu preparo aquém do esperado, tendo em vista tratar-se de uma nação muito dependente do espaço cibernético e ao mesmo tempo possuindo diversas infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) apresentando significativas deficiências na parte de segurança. Seriam necessários mais investimentos no setor e como a área abrange a interação com órgãos públicos e privados, especialmente os órgãos da Administração Pública Federal, os mesmos devem envidar mais esforços para melhorias em sua área de atuação e responsabilidade.

A pesquisa será fundamentada em referência bibliográfica, com abordagem qualitativa, de caráter exploratório. O estudo tem o propósito de analisar as ações desenvolvidas pelo Ministério da Defesa/Exército após a implementação da Estratégia Nacional de Defesa (2008), no contexto da Defesa Cibernética, ou seja, o que vem sendo realizado no país para a efetivação das ações estratégicas referentes à proteção dos sistemas e frente a possíveis ameaças externas. Como objetivos específicos: elencar no contexto mundial, as principais ocorrências relacionadas a ações e ataques cibernéticos dos últimos anos; relacionar os aspectos atuais de defesa cibernética no Brasil, bem como, as estratégias de defesa que vem adotando-se; e ainda, citar algumas das principais ameaças e vulnerabilidades cibernéticas e possíveis soluções para sua resolução/mitigação.

2 Desenvolvimento

A seguir, serão descritos o referencial teórico sobre um sucinto histórico de ações e acontecimentos no meio cibernético, aspectos atuais da Defesa Cibernética Nacional, principais ameaças e vulnerabilidades associadas ao meio cibernético e possíveis formas de mitigação.

2.1 Um breve histórico de ações e acontecimentos no meio cibernético

Atualmente, a sociedade vive a chamada era da informação e merece destaque que, desde os primórdios tecnológicos, ela tem enfrentado situações ou problemas relativos à segurança. A seguir, podem ser verificados alguns dos acontecimentos relativos a ações cibernéticas que tiveram expressivas repercussões.

Segundo War (2010), no ano de 1982, satélites espiões norte-americanos detectaram grande liberação de energia na

Sibéria, sendo que o episódio tratava-se de uma explosão em um gasoduto que, segundo fontes, ocorreu devido ao funcionamento incorreto de seu sistema de controle, sob o comando de um computador. A Agência Central de Inteligência norte-americana (CIA) teria modificado o sistema fazendo o gasoduto realizar operações com pressões muito acima de seus limites ocasionando a explosão.

No ano de 1999, durante o conflito pela autonomia do Kosovo em relação ao governo central da Sérvia, *hackers* sérvios e kosovares entraram em enfrentamento. O fato foi registrado na campanha aérea norte-americana contra alvos da infraestrutura sérvia, essência estratégica do conflito. Depois de a Embaixada da China em Belgrado ser bombardeada acidentalmente, *hackers* chineses também perpetuaram diversos ataques a *sites* do governo norte-americano (MESSMER, 1999).

Em 2000, ocorreu um ataque cibernético a infraestruturas da Austrália. Um ex-funcionário de uma companhia de esgotos, insatisfeito com a preterição para sua promoção, invadiu o sistema de controle de bombas da companhia e causou o derramamento de milhões de litros de esgoto nas ruas da cidade de Maroochy (NUNES, 2010).

Ainda, de acordo com Nunes (2010, p. 93):

> […] em seis de setembro de 2007, Israel realizou um ataque aéreo à Síria, objetivando destruir uma suposta instalação nuclear denominada Al-Kibar, localizada na região de Deir ez-Zor. Algumas fontes afirmam que, para evitar o engajamento de suas aeronaves pelo sofisticado sistema de defesa antiaérea sírio, recém-adquirido da Rússia, este último sofreu um eficaz ataque cibernético que teria mantido o funcionamento aparentemente normal dos equipamentos, que, entretanto, descartaram os contatos gerados pelas aeronaves israelenses.

Ainda em 2007, em retaliação ao governo da Estônia, após o mesmo remover um memorial de guerra da era soviética no centro de sua capital, houve um marcante ataque coordenado de negação de serviço sobre servidores do governo e dos bancos estonianos (WAR, 2010).

Em 2009, houve a criação do Comando de Operação Cibernética nos EUA, que é um comando subunificado das forças armadas, subordinado ao Comando Estratégico dos Estados Unidos (WIKIPÉDIA, 2016). Essa criação demonstra o tamanho da importância que os norte-americanos dão ao assunto e que a doutrina militar americana inclui na sua estratégia o campo de conflito cibernético. O USCYBERCOM, como é chamado, possui uma estrutura de primeiro mundo e está dando passos largos no campo da defesa cibernética americana.

Um *worm* chamado Stuxnet, em 2010, pode ter sido causador de danos às instalações de uma Usina Nuclear localizada no Irã, provocando grandes

prejuízos. Sua disseminação se deu por meio de um *pendrive*, e o objetivo seria atacar sistemas de controles industriais utilizados no monitoramento e execução de grandes instalações, manipulando os equipamentos físicos, de modo a fazê-los agir de forma programada pelo atacante, tornando-se uma verdadeira arma cibernética (KUSHNER, 2013).

De acordo com Symantec (2011), em novembro de 2011, surgiu uma ameaça muito semelhante ao Stuxnet, denominada Duqu. Esta teria objetivo de recolher dados de inteligência e bens de entidades, tais como fabricantes de sistemas de controle industrial, para facilitar a condução de um futuro ataque contra terceiros.

Em junho de 2013, Edward Snowden, ex-funcionário terceirizado da Agência Nacional de Segurança (NSA) dos Estados Unidos, revelou que o seu país espionava dados telefônicos e de internet de muitos países. Segundo informações, o Brasil é o país mais monitorado em toda a América Latina e apenas em janeiro de 2013, foram espionados 2,3 bilhões de telefonemas e mensagens. Setores estratégicos do país, como a Petrobrás e o Ministério de Minas e Energia (MME), além da própria Presidente da República, também foram alvo de espionagem, o que causou na época um descontentamento por parte do governo brasileiro com os Estados Unidos (GREENWALD; KAZ; CASADO, 2013).

Em maio de 2017, ocorreu um grandioso ataque, ocasionado pela invasão de *sites* governamentais do mundo todo, sendo que, no Brasil, organizações como o Ministério Público de São Paulo e o Tribunal de Justiça de São Paulo (TJSP) foram os mais afetados. As máquinas tiveram seus dados criptografados pelo *Malware Ransonware* e houve a exigência de pagamento US$ 300 (trezentos dólares) em *bitcoins* por máquina para a liberação. Nessa ocasião, a Petrobrás, o Instituto Nacional de Segurança Social (INSS) e o Hospital Sírio Libanês também foram afetados (BARROS, 2018).

Em 2019, mensagens privadas do Ex-Ministro da Justiça e Segurança Pública, Sérgio Moro, foram interceptadas e divulgadas, causando enorme constrangimento institucional, tanto a respeito de uma suposta conduta perpetrada pelo ministro enquanto juiz, quanto pela legalidade e moralidade na obtenção de tais diálogos (BARROS, 2018).

Em 2020, de acordo com a empresa Fortinet, o Brasil sofreu mais de 1,6 bilhão de tentativas de ataques cibernéticos no primeiro trimestre do ano, de um total de 9,7 bilhões da América Latina. Tais ações vêm sendo exploradas pela confiança e ingenuidade das pessoas que estão em busca

de informações sobre o COVID-19 (OLHAR DIGITAL, 2020).

Com este histórico de algumas ocorrências cibernéticas, observa-se que a tendência é de que as ameaças cresçam e evoluam cada vez mais, buscando brechas onde possam se estabelecer e assim conseguir êxito em seu propósito. Não só os Estados Unidos, mas também outras economias desenvolvidas, como Reino Unido, Japão, Espanha, Austrália e outras estão revisando ou lançando suas estratégias nacionais de segurança/defesa cibernética, tentando alcançar uma cooperação internacional, criar uma abrangente legislação nacional e internacional, estabelecer normatização, conscientização e treinamento, e cada vez mais, investir na capacitação de recursos humanos especializados.

2.2 Aspectos relevantes e atuais da Defesa Cibernética Nacional

Globalmente, houve muita evolução na área cibernética, mas ainda há muito a se fazer. Na atualidade, a maioria dos países, mesmo que de forma modesta, tem uma estrutura de defesa cibernética. Em grande parte o organograma e estrutura são bem parecidos com o sistema Brasileiro, que fica a cargo do Ministério da Defesa, órgão responsável pela coordenação das atividades (BRASIL, 2014).

A preocupação atual, não só das grandes potências mundiais, mas também dos demais países, incluindo o Brasil, deve ser maior com as infraestruturas estratégicas, tais como: hidrelétricas, gasodutos, plataformas de petróleo, usinas nucleares, sistemas de controle aéreo, controle de trafego de veículos, sistemas de telefonia, sistemas militares, etc., que são de grande importância estratégica e fundamentais ao desenvolvimento nacional. Um mau funcionamento ou inoperância destas podem vir a paralisar completamente o país causando diversas calamidades. A essas instalações, devido ao seu grau de importância e criticidade, são chamadas de Infraestruturas Críticas (MANDARINO; CANONGIA, 2010).

Dentro do contexto internacional de muitas ocorrências cibernéticas e de uma remota, mas não impossível guerra, os países mais influentes perceberam a oportunidade de vantagem do emprego de armas cibernéticas nos teatros de operação. Todas as nações devem acreditar na possibilidade de ser alvo, em futuro próximo, de ataques cibernéticos.

Esta “guerra” é silenciosa, mas pode gerar grandes perdas materiais, quando não catástrofes político-sociais ou humanas. Por isso é importante conhecer o grau de vulnerabilidade do país, com relação aos diversos sistemas e às infraestruturas críticas de informação, bem como conceber

um sistema eficaz de medidas preventivas e de respostas contra ataques cibernéticos (MANDARINO; CANONGIA, 2010).

Segundo Barros et al. (2011), no Brasil, não se tem relatos oficiais de ataques cibernéticos contra as infraestruturas críticas. O chamado "apagão elétrico", ocorrido no fim de 2009, deixou quatro estados do Brasil completamente sem fornecimento elétrico e outros 14 foram parcialmente afetados, sendo especulado como um possível caso de ataque aos sistemas de computadores de controle da rede elétrica, o que, efetivamente, não foi comprovado. Porém, recentemente, um dos efeitos colaterais da pandemia de coronavírus foi um aumento no número de ataques cibernéticos, principalmente contra empresas do setor elétrico no Brasil e no exterior. Nesse contexto, empresas como a Energisa e Light e as europeias Enel e EDP foram atingidas por criminosos virtuais (REUTERS, 2020).

Não só as ameaças lógicas demandam preocupação no ciberespaço, mas também as ameaças físicas que podem colocar em risco ativos primordiais. Segundo War (2010), verifica-se que mais de 90% do tráfego da internet passa por fibras óticas em cabos submarinos, os quais, ao longo de seus trajetos, por vezes se concentram perigosamente em alguns pontos de estrangulamento, como, por exemplo, ao largo de Nova Iorque, no Mar Vermelho e no Estreito de Luzon, nas Filipinas.

No Brasil, temos como pontos importantes as águas localizadas próximas às cidades do Rio de Janeiro, de Santos e de Fortaleza, conforme mostrado na figura 1.

Figura 1 – Distribuição dos cabos submarinos de fibra ótica

Fonte: WAR (2010, p.26)

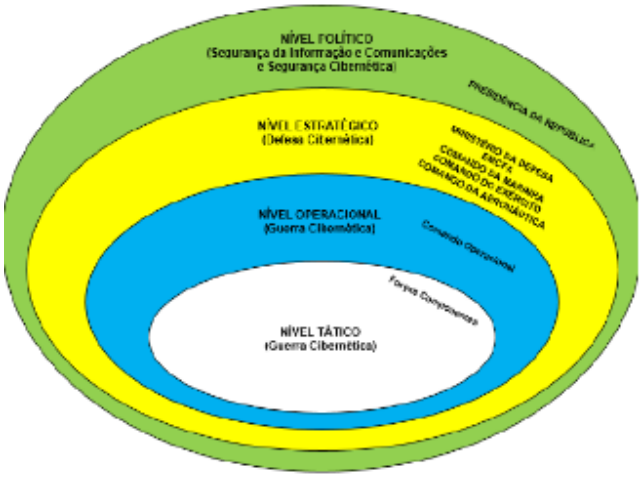
Devido à importância do tema, a Estratégia Nacional de Defesa de 2008 (END) definiu três setores fundamentais para a Defesa Nacional: o nuclear, a cargo da Marinha do Brasil; o espacial, a cargo da Força Aérea Brasileira; e o cibernético, a cargo do Exército Brasileiro (EB). Desde então, o Exército tem atuado no assunto em questão, de forma a melhorar os aspectos ligados à proteção de nossas infraestruturas. Segundo a Estratégia Nacional de Defesa:

> As capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar (BRASIL, 2008).

A partir da publicação da END, muita coisa evoluiu e o assunto foi mais explorado no âmbito governamental, havendo implementação de diversas diretrizes, decretos e portarias. Houve inclusive a criação de vários órgãos com a finalidade de exercer atividades de Segurança Cibernética e de Segurança da Informação e Comunicações na Administração Pública Federal, como por exemplo, o Núcleo do Centro de Defesa Cibernética, ativado em 02 de agosto de 2010. Cita-se também, em 20 de setembro de 2012, a mudança na Estrutura Regimental do Comando do Exército, sendo incluído o Centro de Defesa Cibernética (CDCiber).

A figura 2 mostra a atual organização estrutural do Sistema Brasileiro de Defesa Cibernética na Doutrina Militar de Defesa Cibernética, aprovada pela Portaria Normativa 3.010/MD, de 18 de novembro de 2014, expressando as responsabilidades com relação ao nível de decisão no contexto do Ministério da Defesa.

Figura 2 – Estrutura e nível de decisão atual (Doutrina Militar de Defesa Cibernética)



Fonte: BRASIL (2014, p.17)

Observa-se que segundo a Doutrina Militar de Defesa Cibernética, Brasil (2014, p.17), conhecida como MD31-M-07, as ações atuais no ciberespaço têm as seguintes definições sob a luz do Ministério da Defesa:

> Nível político - Segurança da Informação e Comunicações e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo a Administração Pública Federal direta e indireta, bem como as Infraestruturas Críticas da Informação Nacionais;
> Nível estratégico - Defesa Cibernética - a cargo do Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas e Comandos das Forças Armadas, interagindo com a Presidência da República e a Administração Pública Federal; e
> Níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das Forças Armadas.

Segundo a MD31-M-07, na prática, os tipos de ações cibernéticas são ataque, proteção e exploração, e com relação às formas de atuação seguem o esquema proposto no quadro 1.

Quadro 1 – Formas de atuação cibernética

FORMA DE ATUAÇÃO CIBERNÉTICA / CRITÉRIOS	POLÍTICA / ESTRATÉGICA	OPERACIONAL / TÁTICA
Nível dos Objetivos	Políticos e/ou Estratégicos	Operacionais e/ou Táticos
Foco	Obtenção de Inteligência	Preparação do campo de batalha
Nível de envolvimento nacional	Normalmente interministerial, podendo requerer ações diplomáticas e de vários ministérios e agências (Defesa, Relações Exteriores, Ciência, Tecnologia e Inovação, GSI/PR, Agência Brasileira de Inteligência - ABIN, Agência Nacional de Telecomunicações - ANATEL etc.)	Normalmente no âmbito do Ministério da Defesa, podendo contar com apoio do Ministério das Relações Exteriores
Contexto	Desde o tempo de paz, podendo fazer parte de uma Operação de Informação ou de Inteligência	Em um ambiente de crise ou conflito, apoiando uma ação militar
Nível tecnológico empregado	Normalmente alto ou muito alto	Normalmente médio ou baixo
Sincronização	Dentro do contexto de uma sofisticada Operação de Inteligência, podendo requerer ações diplomáticas anteriores ou posteriores	Dentro do contexto dos sistemas operacionais de uma Operação Militar, sincronizado com a manobra
Tempo de Preparação e Duração	Duração prolongada, com tempo de preparação normalmente mais longo, com desenvolvimento e emprego de técnicas de difícil detecção	Duração limitada, normalmente com moderado ou curto tempo de preparação, utilizando conhecimentos já levantados e técnicas previamente preparadas

Fonte: BRASIL (2014, p.23)

Ainda no âmbito militar de defesa cibernética e visando criar *expertise* para este assunto tão importante, foram criados pelo Exército Brasileiro os cursos de Guerra Cibernética para Sargentos (CGCIBER SGT) e de Guerra Cibernética para Oficiais (CGCIBEROF). Os referidos cursos são

administrados pelo Centro de Instrução de Guerra Eletrônica (CIGE), localizado em Brasília-DF, tendo por finalidade habilitar profissionais para ocupar cargos e desempenhar funções de segurança, defesa e guerra cibernética nas diversas organizações militares ligadas a área e de interesse do Comando do Exército, além de atender às necessidades de recursos humanos do Exército e do Ministério da Defesa. O CIGE, primeiro centro de treinamento de Guerra Eletrônica da América Latina, foi criado pelo Decreto Presidencial n° 89445, de 19 de março de 1984, e é considerada organização pioneira do Exército Brasileiro, no assunto Guerra Cibernética (COMANDO DE COMUNICAÇÕES E GUERRA ELETRÔNICA DO EXÉRCITO, 2013).

Atualmente, o EB conta ainda com um Simulador Nacional de Operações Cibernéticas (SIMOC). É desenvolvido com tecnologia nacional, tratando-se de uma tecnologia de virtualização baseada em cenários realistas (desastres, comprometimento de estruturas críticas, etc) e que tem a missão de ajudar as tropas brasileiras em treinamentos contra uma possível guerra cibernética. O *software* faz parte do programa de Estratégia da Defesa Nacional do Comando de Comunicações e Guerra Eletrônica do Exército (CComGEx), e através dele, se dá o treinamento e especialização de recursos humanos para a análise de vulnerabilidades de redes, de modo a possibilitar a adoção de ações de proteção e defesa ativa. Com o SIMOC tem-se ainda a possibilidade de verificação da eficácia e eficiência das ações, através da utilização de métricas (COMANDO DE COMUNICAÇÕES E GUERRA ELETRÔNICA DO EXÉRCITO, 2013).

Outra importante ação a ser citada é o antivírus DefesaBR (tecnologia nacional), desenvolvido pela empresa BluePex, e que foi uma das primeiras soluções empregadas pelo Exército na melhoria da segurança de seus dispositivos. Mais recentemente, o Centro de Desenvolvimento de Sistemas do Exército (CDS), com apoio técnico e administrativo do CITEx (Cento Integrado de Telemática do Exército), especificou e licitou, uma nova solução corporativa de antivírus para o Exército, baseada na solução comercial Karspersky.

Neste ano, o governo publicou, no Diário Oficial da União, a Estratégia Nacional de Segurança Cibernética (E-Ciber), visando tornar o Brasil um país seguro, proteger o espaço cibernético, aumentar a resiliência do país aos ataques cibernéticos e fortalecer a atuação brasileira em segurança *online* no cenário internacional. Nessa estratégia estão previstas uma dezena de ações, tais como, a criação de fóruns de governança, adoção de soluções nacionais de criptografia e a

adequação de uma legislação específica (OLHAR DIGITAL, 2020).

Com isso, observa-se que o Ministério da Defesa, através das Forças Armadas Brasileiras, está cada vez mais empregando recursos tecnológicos e efetuando ações, na procura por um ambiente cibernético melhor protegido das crescentes ameaças. Com relação a este vultoso assunto em âmbito nacional, Mandarino e Canongia (2010, p. 11) afirmam:

> Sabemos que ainda há muito a ser alcançado, pois estamos dando os primeiros passos, para criar as condições necessárias de segurança cibernética, principalmente, no que diz respeito ao entendimento das novas exigências para a proteção da sociedade e do Estado Brasileiro. Esta é uma realidade que deve estar presente nas agendas do governo, da academia, do setor privado, e do terceiro setor, não somente como um desafio do país, mas como um desafio de magnitude mundial. Salientamos que o país, apesar de estar construindo as bases de sua Política no tema, já vem sendo reconhecido internacionalmente como um dos protagonistas. Ressaltamos que criar, cultivar e ampliar a cultura de segurança cibernética no Brasil, é um desafio de longo prazo e de grande alcance, que merece um olhar especial.

Por fim, a preocupação constante com aspectos ligados à segurança da informação é um dever de todos os países do globo. Conforme Paludeto (2011), na nova geração de conflitos, o espaço cibernético é um novo ambiente operacional cujas possibilidades são imensuráveis, fazendo com que haja uma maior preocupação com atividades de ataque e defesa para as diversas nações.

2.3 Principais ameaças e vulnerabilidades associadas ao meio cibernético e possíveis formas de mitigação

Vulnerabilidade é uma fragilidade presente ou associada a ativos que manipulam ou processam informações, que ao ser explorada por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios de segurança da informação. Por si só não provoca incidentes, uma vez que se trata de elementos passivos, que necessitam de um ocasionador ou uma situação propícia que são as ameaças (SÊMOLA, 2003).

Já ameaça é um agente ou potencial que causa incidentes e viola a segurança, por meio da exploração de vulnerabilidades, ou quando há uma circunstância, capacidade, ação favorável para isso. Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade (SÊMOLA, 2003).

A verificação das vulnerabilidades e ameaças é fundamental para estabelecer a segurança de um sistema ou de uma rede. Nesse intuito a análise de vulnerabilidades verifica a existência de falhas de segurança no ambiente computacional das organizações, implementando assim controles de segurança eficientes sobre os ativos. É realizada através de um

levantamento minucioso do ambiente de tecnologia da informação, verificando se o mesmo tem as condições de segurança necessárias, levando em conta a importância estratégica dos serviços que a organização fornece ou desempenha.

Entende-se por risco como a probabilidade de que uma ameaça explore vulnerabilidades em um determinado ativo, comprometendo assim a sua segurança, estando sempre associados à ocorrência de algum incidente (SÊMOLA, 2003). No Brasil, quando comparado com países mais desenvolvidos, poucas organizações tratam eficientemente os riscos em seus negócios. Como regra geral, deveria haver uma análise meticulosa dos riscos existentes e uma estratégia de tratamento/mitigação dos mesmos.

Dentre os benefícios de uma adequada gestão de riscos estão: melhora a eficácia e efetividade das decisões para controlar riscos nos processos internos e externos e suas interações; possibilita mapear os riscos associados com o negócio e a gestão da informação, mantendo a imagem e reputação da organização; minimiza as possibilidades de furto de informação e maximiza a proteção de dados; estabelece adequação e conformidade com os requisitos legais e regulatórios.

Conforme Basso (2010), na velocidade em que novas aplicações são desenvolvidas atualmente, muitas falhas de segurança são verificadas e reportadas por empresas especializadas. Estas falhas que muitas vezes trazem enormes prejuízos, sem sombra de dúvidas, são decorrentes geralmente das árduas restrições de tempo e custo do desenvolvimento.

Sabendo destas falhas pessoas mal intencionadas podem efetuar ataques com o intuito de causar danos aos serviços e ativos, tentando explorar suas vulnerabilidades. Existem vários tipos de ataques que podem explorar estas falhas e serem utilizados contra uma organização, empresa, e até mesmo em uma infraestrutura crítica. Conforme Stallings (2008), a intrusão não autorizada em um sistema ou redes de computadores é uma das ameaças mais sérias à segurança. O objetivo do intruso é entrar no sistema, obtendo acesso às informações que deveriam estar protegidas e de acesso restrito a algumas poucas pessoas autorizadas.

Desde o surgimento das primeiras ameaças, a procura por mecanismos de segurança tem aumentado significativamente, e para isso são utilizados equipamentos, *softwares*/ferramentas, estratégias ou ainda as chamadas políticas de segurança. No campo da segurança de aplicações *web*, o *Open Web Application Security Project* (OWASP), ou Projeto Aberto de Segurança

em Aplicações Web, é uma comunidade *online* que cria e disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias e que tem como um dos seus projetos o OWASP Top 10.

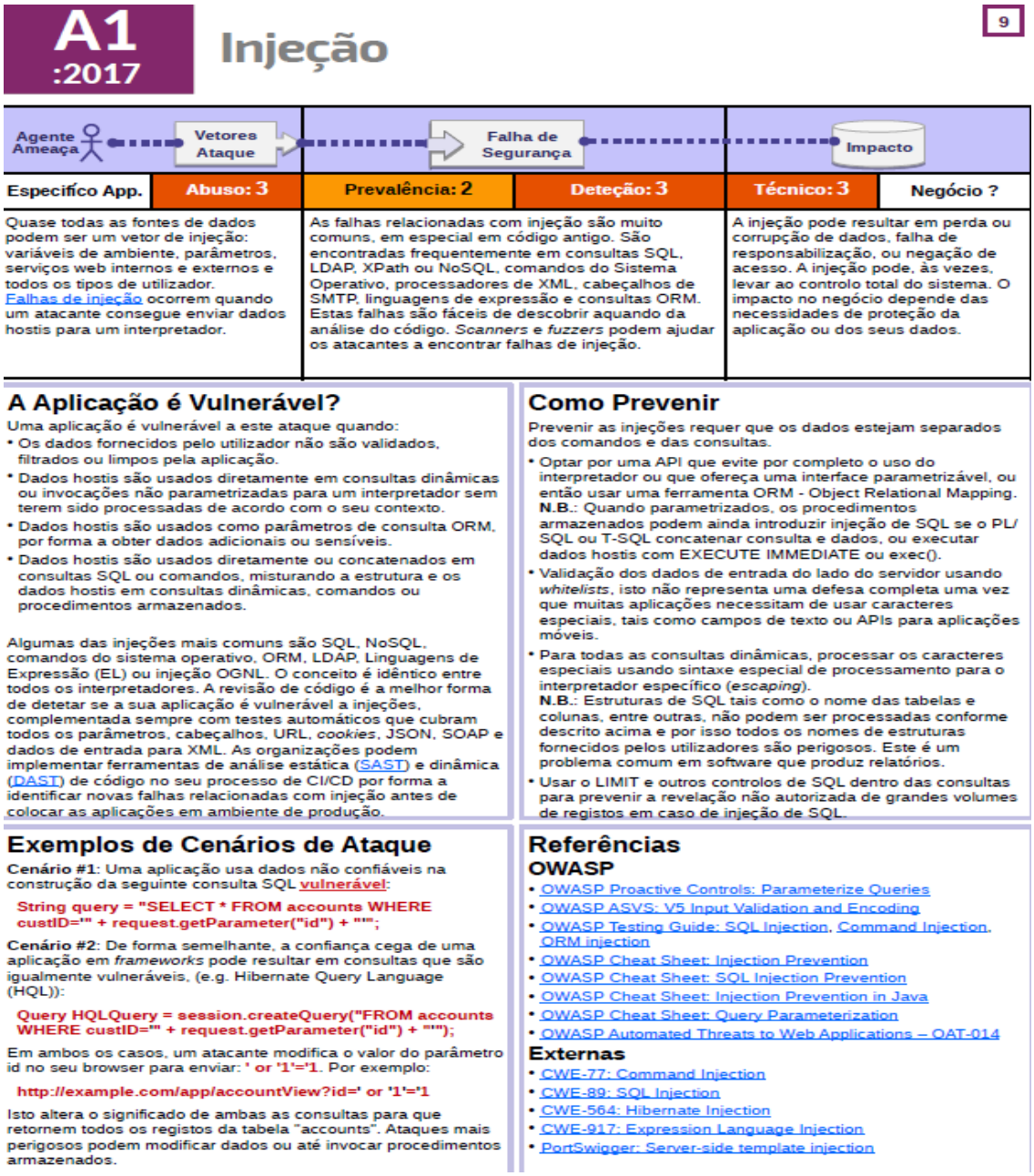
O objetivo principal do OWASP Top 10 é educar desenvolvedores, projetistas, arquitetos, gestores e organizações sobre as consequências das mais importantes vulnerabilidades de segurança de aplicações *web*, fornecendo maneiras de se proteger das ameaças existentes. Na figura 3 são listados, segundo a OWASP TOP 10 (2017, p. 8), as dez maiores vulnerabilidades em aplicações *web*.

Figura 3 – Vulnerabilidades em aplicações *WEB*

Fonte: OWASP TOP 10 (2017, p. 8)

Esse mesmo Top 10 lista algumas formas de evitar as vulnerabilidades citadas, trazendo algumas informações para saber se sua aplicação está vulnerável, exemplos de cenário de ataque, referências da própria OWASP e outras externas relacionadas ao assunto, que podem agregar mais conhecimento na melhoria da segurança. A contramedida mostrada na figura 4 é referente à ameaça de injeção (A1), que é uma das mais exploradas nos dias atuais.

Figura 4 – Contramedida de injeção em aplicações *WEB*



Fonte: OWASP TOP 10 (2017, p. 9)

Este projeto trata-se de um documento bem completo e interessante, sendo indispensável aos gestores de segurança da informação, o seu conhecimento e aplicação no ambiente de tecnologia da informação das organizações desenvolvedoras.

Ainda no contexto de aplicações *Web* e para estabelecer uma maior segurança no ciclo de vida do desenvolvimento, o OWASP recomenda que, para a melhoria dos processos, se utilize o Modelo de Maturidade de Garantia do Software (SAMM). Trata-se de um *framework* aberto e pertencente à OWASP, que ajuda a formular e implementar estratégias para a segurança do software, feita de forma personalizada para os riscos enfrentados.

Em computadores de uso comum, e até mesmo servidores, se não houver nenhum tipo de proteção, é comum que algum *malware* tente se estabelecer. De acordo com Cert.br (2016), m*alwares* são todos os tipos de programas /*softwares*/códigos desenvolvidos com a finalidade de executar ações maliciosas em um computador podendo afetar o mesmo. Abaixo alguns exemplos de *malwares* segundo Cert.br (2016):

- Vírus - São todos os artefatos de software que executam funções não desejáveis. Possuem ainda a capacidade de se reproduzir, porém, necessitam de um vetor para propagação;
- *Trojans* - Também chamados Cavalos de Tróia, apresentam características de software inofensivo, mas quando acionado possibilita ao atacante assumir o controle do dispositivo;
- *Backdoor* - Programa que possibilita o invasor retornar a um dispositivo ou sistema comprometido, por meio da modificação do funcionamento normal do mesmo.
- *Worms* - Os *worms*, ou vermes, se propagam facilmente e podem se espalhar pelas diversas formas existentes. Reúne características dos vírus e dos *trojans*, mostrando-se bastante versátil e de rápida disseminação;
- *Bot* - programa com características semelhantes ao *worm* possuindo ainda mecanismos de comunicação com o atacante que consegue controlá-lo remotamente.
- *Spywares* - Os programas espiões são tipos de *malware* criados para coletar informações de uma ou mais atividades da máquina atacada, repassando as informações coletadas ao atacante;
- *Keyloggers* - São tipos de *spywares* utilizados para monitorar atividades do teclado da máquina atacada, transmitindo ou armazenando as

informações coletadas, de forma que o atacante consiga acessá-las posteriormente;

- *Rootkits* **-** Conjunto de ferramentas utilizadas por um atacante para ter controle da máquina atacada. Com a utilização de técnicas de ocultação dos rastros de comprometimento se mantêm de forma sigilosa;
- *Ransonware* - Tipo de *malware* que restringe o acesso ao computador da vítima (criptografia) e cobra um valor em dinheiro pelo resgate.

Na luta contra estes artefatos maliciosos, identifica-se o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, conhecido como CERT.br, e que é mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. O CERT.br trata incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira, atuando também através do trabalho de conscientização sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet brasileira e do auxílio ao estabelecimento de novos Grupos de Resposta a Incidentes de Segurança em Computadores (CSIRTs) no Brasil.

Segundo Cert.br (2016), algumas medidas possíveis contra os *malwares* e outras ameaças são:

- Manter seus dispositivos atualizados: use apenas *softwares* originais, tendo sempre as versões mais recentes instalados; instale todas as atualizações, principalmente as de segurança; crie um disco de recuperação para uso em caso de necessidade.

- Instalar um antivírus (antimalware): mantenha o antivírus atualizado diariamente, incluindo o arquivo de assinaturas; padronizar os antivírus para verificar automaticamente, antes de abrir ou executar, toda e qualquer extensão de arquivo recebido, arquivos anexados aos e-mails, obtidos pela Internet e os discos rígidos e as unidades removíveis; não utilizar simultaneamente diferentes antivírus, pois eles podem entrar em conflito, afetar o desempenho do equipamento e interferir na capacidade de detecção um do outro; crie um disco de emergência de seu antivírus e use-o se desconfiar que o antivírus instalado esteja com funcionamento incorreto.

- Usar um *firewall* pessoal: Sobre este dispositivo: "[...], *firewall* é um termo utilizado para identificar um conjunto de sistemas e equipamentos que implementam mecanismos de proteção de perímetro entre redes." (BARBOSA, 2006, p. 24). Sabendo disso, assegure-se de ter um *firewall* pessoal instalado e ativo e procure analisar periodicamente os *logs* do mesmo à procura de acessos maliciosos.

- Ter uma política de registro de eventos (*logs*): Sendo úteis no monitoramento, detecção e resolução de problemas dos usuários, o *log* é um arquivo onde são registrados e armazenados os eventos que ocorrem em um sistema ou rede. Cada entrada de registro contém informações relacionadas a um evento específico que tenha ocorrido neste sistema ou rede. Conforme o Núcleo de Informação e Coordenação do Ponto BR:

> Logs são muito importantes para a administração segura de sistemas, pois registram informações sobre o seu funcionamento e sobre eventos por eles detectados. Muitas vezes, os logs são o único recurso que um administrador possui para descobrir as causas de um problema ou comportamento anômalo (NIC.BR, 2003).

- Ao fazer instalação de aplicativos: Usar somente os de fontes confiáveis, que sejam bem avaliados e com grande quantidade de usuários, observando se as permissões de instalação e execução são coerentes.

- Fazer *backups*: Faça *backups* regularmente ou de acordo com a necessidade da organização, mantendo os fisicamente em locais seguros. Nunca recupere um *backup* se desconfiar que ele possua dados não confiáveis e mantenha os mesmos desconectados do sistema evitando assim acessos indevidos.

- Ser cuidadoso ao clicar em *links*: não considere que mensagens de remetentes conhecidos são sempre confiáveis, pois o campo de remetente do e-mail pode ter sido falsificado, ou elas podem ter sido enviadas de contas falsas ou invadidas. Antes de acessar um *link* curto procure usar recursos que permitam visualizar o real *link* de destino.

- Usar a técnica de *System hardening*: Sempre que possível ou necessário, os administradores devem usar deste importante processo para fortalecer a segurança dos dispositivos. Segundo Reis et al. (2012, p. 21):

> O *hardening* consiste na realização de alguns ajustes finos para o fortalecimento da segurança de um sistema. Muitos administradores sem experiência em segurança preparam seus servidores com uma instalação básica e depois que suas aplicações estão disponíveis nenhum procedimento é feito para manter a integridade do sistema.

- Quando necessário utilizar sistemas de detecção e de prevenção de intrusão (IDS/IPS): Os *Intrusion Detection System* (IDS), ou Sistemas de Detecção de Intrusão tem a função de monitorar o tráfego em uma rede. Suas ações são reativas, pois não interferem no tráfego da rede. Os IDS devem ser rápidos, pois quanto mais cedo o intruso for detectado e expulso do sistema, menos danos ele irá causar. Já os Sistemas de Prevenção de Intrusão, ou *Intrusion Prevention System* (IPS) bloqueiam um ataque na rede a partir do seu primeiro pacote, o que pode ser fundamental para neutralizá-lo. Os IPS exigem grande capacidade de

processamento para poder analisar todos os pacotes que passam por ele, podendo causar lentidão na rede (STALLINGS, 2008).

- Outras ações: Estabelecer uma boa política com senhas (senhas fortes e exigência de mudança periódica); utilizar a conta de administrador apenas quando necessário; cuidado com extensões ocultas, pois alguns sistemas possuem como configuração padrão, ocultar a extensão de tipos de arquivos conhecidos; desabilite a auto-execução de mídias removíveis e de arquivos anexados; no caso de empresas e organizações, eduque seus funcionários de acordo com uma política de segurança, abordando sempre o tema com eles e evitando assim, ataques de engenharia social.

Considerando-se risco a possibilidade de sofrer danos ou perdas, o gerenciamento dos mesmos envolve a sua identificação, sua avaliação e a tomada de medidas para reduzi-los. Portanto, este gerenciamento pode ser dividido em avaliação e tratamento. Usa-se a avaliação de risco para saber a extensão da ameaça potencial e o risco relacionado aos seus serviços. Como resultado, tem-se a identificação dos controles para reduzir ou eliminar o risco, os quais deverão ser os mais adequados para conseguir reduzir o risco ao nível aceitável, com o menor custo e proporcionando o menor impacto negativo aos recursos e funcionalidades da organização (SÊMOLA, 2003).

Conforme Stoneburner et al. (2002), a mitigação de riscos refere-se à redução da possibilidade de fracasso por meio do mapeamento dos processos e da implementação de políticas ou regras para os procedimentos, estando associada à etapa de tratamento de riscos. Está relacionada à priorização, avaliação e implementação dos controles de segurança recomendados na avaliação de risco e ocorre, inicialmente, através da análise de eventos maliciosos, a qual torna possível a adoção de medidas que visam reduzir e/ou eliminar riscos, objetivo principal nesta atividade.

Ainda na busca por um ambiente organizacional mais seguro, existem diversas normas, frameworks e ferramentas, que ajudam os profissionais de Tecnologia da Informação das organizações, a melhorar e implantar políticas/controles relativos à segurança de informação. Como exemplo, cita-se a área de conhecimento de gerenciamento de riscos de projetos, do conjunto de práticas na gestão de projetos organizado pela instituição internacional *Project Management Institute* (PMI), conhecido como guia *Project Management Body of Knowledge* (PMBOK). Citamos também, dentre outras normas, as da família ISO 27000, especialmente a norma ISO/IEC 27002, que estabelece o código de melhores práticas para apoiar a implantação

do Sistema de Gestão de Segurança da Informação (SGSI) nas organizações, recomendando os requisitos necessários para o estabelecimento da segurança da informação.

Sabendo das vulnerabilidades e ameaças existentes e o risco associado às mesmas, um bom profissional de Segurança da Informação, pode estabelecer medidas necessárias, com a finalidade de prevenir que seus sistemas computacionais não sejam afetados. Esse acompanhamento ou gestão da segurança da informação deve ser diuturno, face às evoluções constantes da tecnologia e o surgimento de novas brechas.

3 Conclusão

Neste artigo foram abordados alguns aspectos referentes à Defesa Cibernética nacional, possibilitando ver a evolução do assunto, esclarecer o funcionamento/organograma atual com suas respectivas responsabilidades e atividades desenvolvidas pelas organizações frente ao tema. O presente artigo visa contribuir no esclarecimento de algumas informações referentes a temática e conscientizar/incentivar as pessoas em relação aos cuidados e boas práticas/ações nos aspectos relacionados a Defesa Cibernética.

Atualmente, todas as nações já tomaram conhecimento, algumas na prática, da importância da proteção do seu espaço cibernético e de suas infraestruturas fundamentais. As mais desenvolvidas estão na vanguarda, se tornando um padrão de fato para outros países menos desenvolvidos nesse quesito.

No Brasil, o setor cibernético alavancou depois da publicação da END 2008, sendo o marco para o seu desenvolvimento no país, havendo após esse fato, uma implementação de diversos projetos e uma maior preocupação com o estabelecimento de uma visão de futuro cibernética e a proteção de infraestruturas críticas nacionais. Setores públicos e privados dedicaram-se mais a temática e investiram grandes recursos, obtendo recursos humanos dotados de alta competência técnica e parque tecnológico especializado e atualizado, alcançando assim uma verdadeira revolução.

Ao longo da pesquisa apresentou-se algumas ameaças e vulnerabilidades existentes e foram relacionadas algumas soluções para mitigá-las/saná-las. Observa-se que elas crescem e evoluem juntamente com as novas tecnologias, obtendo cada vez mais complexidade e alcance inimagináveis, tornando árduo e incerto o processo de prevenção e de mitigação. A melhor maneira de se lidar com isso, é se preparando para evitá-las, ou quando não possível, mitigá-las.

Nos últimos anos, o Brasil evoluiu muito nesse ambiente revolucionário que é

o meio cibernético. Na América do Sul, desponta na vanguarda em assuntos de segurança e defesa cibernética, porém, quando comparado às grandes potências, nosso país ainda precisa melhorar muito em vários aspectos, confirmando a hipótese de que necessita de muitos investimentos no setor, mais prioridade nas pautas do Governo e estabelecimento de melhores mecanismos de proteção das infraestruturas críticas, não estando totalmente preparado para este novo desafio. Para a segurança, evolução e melhoria contínua do espaço cibernético brasileiro, faz-se necessário uma preocupação diuturna, não só por parte dos governantes, militares e acadêmicos, mas também de toda sociedade, pois somente com o apoio e conscientização de todos pode-se garantir a soberania cibernética nacional.

Saber gerir as infraestruturas de tecnologia da informação, através dos sistemas de gestão e planejamento, das ferramentas de segurança informatizadas e dos meios tecnológicos integrados disponíveis, se torna um fator de sucesso para qualquer organização. As políticas de segurança da informação devem sempre contemplar regras visando à utilização da tecnologia sem o comprometimento da segurança.

Prevenção de forma pró-ativa, conscientização, treinamento, capacitação, seguir as normas referentes ao assunto, melhoria e uso da tecnologia nacional, interação/integração das agências de inteligência nacionais e internacionais com o setor empresarial e universitário, criando um espírito colaborativo na sociedade, são fundamentais para todos os envolvidos, além de mapear/mitigar/sanar os riscos existentes e assim promover uma utilização mais segura do meio cibernético.

Ao ter uma mentalidade voltada para Segurança da Informação, mantendo em foco a preocupação com as ameaças e vulnerabilidades, todos os cidadãos e organizações (sejam órgãos públicos ou privados) tornarão nossas redes e infraestruturas críticas menos impostas a ações cibernéticas maliciosas, que ao serem executadas podem, sem sombras de dúvidas, causar uma calamidade pública. Seguindo estes passos teremos uma nação cada vez mais conceituada a nível mundial e haverá um crescente aumento no grau de confiança do Sistema de Segurança e Defesa Cibernética Nacional.

Por fim, o trabalho limitou-se em explorar as ações desenvolvidas no âmbito Ministério da Defesa/Exército Brasileiro, não abrangendo outras implementações, possivelmente desenvolvidas, em órgãos da Administração Pública Federal ou Estadual. Como perspectiva de trabalhos futuros, poderia ser verificado as ações efetuadas no âmbito dos governos estaduais, ou ainda, em empresas ou organizações consideradas

estratégicas para o Brasil, como as dos setores de energia/telecomunicações e outras denominadas pertencentes as infraestruturas críticas.

REFERÊNCIAS

BARBOSA, A. N. **Um sistema para análise ativa de comportamento de *firewall*.** 2006. 104 f. Dissertação de Mestrado apresentada à Escola Politécnica da Universidade de São Paulo, São Paulo, 2006.

BARROS, O.R.; GOMES, U.M.; FREITAS, W. L.; LACERDA, W. **Desafios estratégicos para segurança e defesa cibernética.** Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

BARROS, Leonardo. 2018: O ano da evolução dos ataques cibernéticos. **Canaltech**. Disponível em: https://canaltech.com.br/seguranca/2018-o-ano-da-evolucao-dos-ataques-ciberneticos-107168/. Acesso em: 01 ago. 2020.

BASSO, T. **Uma Abordagem para Avaliação da Eficácia de Scanners de Vulnerabilidades em Aplicações Web.** 2007. 121 f. Dissertação de Mestrado apresentada à Faculdade de Engenharia Elétrica e de Computação. Área de concentração: Engenharia de Computação, UNICAMP, Campinas – SP, 2010.

BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato20072010/2008/Decreto/D6703.htm>. Acesso em: 01 ago. 2020.

BRASIL. Ministério da Defesa. Portaria normativa nº 3.010/MD, de 18 de novembro de 2014. 1ª ed. 2014. 38p.

CANALTECH. **Número de ataques cibernéticos no Brasil quase que dobrou em 2018**. 2018. Disponível em: < https://canaltech.com.br/seguranca/numero-de-ataques-ciberneticos-no-brasil-quase-que-dobrou-em-2018-119600/>. Acesso em: 01 ago. 2020.

CERT.br. **Fascículo Códigos Maliciosos**. In: Cartilha de Segurança para Internet, 2016. Disponível em: <http://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf>. Acesso em: 01 ago. 2020.

COMANDO CIBERNÉTICO DOS ESTADOS UNIDOS. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2016. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Comando_Cibern%C3%A9tico_dos_Estados_Unidos&oldid=45157626>. Acesso em: 01 ago. 2020.

COMANDO DE COMUNICAÇÕES E GUERRA ELETRÔNICA DO EXÉRCITO. Centro de Instrução de Guerra eletrônica. 2013. Disponível em: <http://www.ccomgex.eb.mil.br/index.php/centro-instrucao-guerra-eletronica>. Acesso em: 01 ago. 2020.

GREENWALD, G; KAZ, R; CASADO, J. **EUA espionaram milhões de e-mails e ligações de brasileiros.** O Globo, Rio de Janeiro, 06 julho 2013. Disponível em: <http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>. Acesso em: 01 ago. 2020.

KUSHNER, D. The real story of Stuxnet**. IEEE Spectrum**. 2013. Disponível em: <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>. Acesso em: 01 ago. 2020.

MANDARINO JR, R; CANONGIA, C. **Livro Verde: Segurança Cibernética no Brasil**. Brasília, GSI/PR: 2010. 63 p.

MESSMER, E. Kosovo cyber-war intensifies**. Network World Fusion**, 1999. Disponível em: <http://www.networkworld.com/news/1999/0512kosovo.html>. Acesso em: 01 ago. 2020.

NIC BR Security Office. **Práticas de Segurança para Administradores de Redes Internet.** Versão 1.2., maio. 2003. Disponível em: <http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html>. Acesso em: 03 ago. 2020.

NUNES, L. A. R. **Guerra cibernética: está a MB preparada para enfrentá-la?** 2010. 98 f. Trabalho de Conclusão de Curso - Curso de Política e Estratégia Marítimas, Escola de Guerra Naval, Rio de Janeiro, 2010.

OLHAR DIGITAL. **Brasil teve mais de 1,6 bilhão de ataques cibernéticos em três meses.** 2020. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/brasil-teve-mais-de-1-6-bilhao-de-ataques-ciberneticos-em-tres meses/100420>. Acesso em: 03 ago. 2020.

OLHAR DIGITAL. **Governo cria estratégia para enfrentar ataques cibernéticos.** 2020. Disponível em: <https://olhardigital.com.br/noticia/governo-cria-estrategia-para-enfrentar-ataques-ciberneticos/96407>. Acesso em: 04 ago. 2020.

OWASP Foundation. **Os dez riscos de segurança mais críticos em aplicações WEB.** Versão: português (Brasil). 2017. Disponível em: < http://www.owasp.org>. Acesso em: 05 ago. 2020.

PALUDETO, V. L**.** Estágio de Guerra Cibernética para Cadetes**. Sangue Novo**. Resende, n. 21, p. 40, ago. 2011.

RATTRAY, G.J. ***Strategic Warfare in Cyberspace***. 1. ed. Massachussets: Cambridge, 2001.

REIS, F. A.; JULIO, E. P.; VERBENA, M. F. Hardening: Blindando um Sistema GNU/LINUX**. Infra Magazine.** São Paulo, jun, 2011. Disponível em: <http://www.devmedia.com.br/websys.4/webreader.asp?cat=62&revista=inframagazine_1#a-3403>. Acesso em: 06 ago. 2020.

REUTERS. **Ataques cibernéticos aumentam com pandemia e atingem companhias elétricas no Brasil e no mundo.** 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/07/03/ataques-ciberneticos-aumentam-com-pandemia-e-atingem-companhias-eletricas-no-brasil-e-no-mundo.ghtml>. Acesso em: 07 ago. 2020.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva da segurança da informação.** 9ª reimpressão. Rio de Janeiro: Elsevier, 2003

SYMANTEC Corporation. **Relatório Cybercrime**. Disponível em: <http://br.norton.com/cybercrimereport/promo>. Acesso em: 01 ago. 2020.

STALLINGS, W. **Criptografia e segurança de redes – Princípios e práticas**. 4. ed. São Paulo: Pearson Prentice-Hall, 2008.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. Risk Management Guide for Information Technology Systems. **NIST - National Institute of Standards and Technology**, Gaithersburg, july. 2002. 54 p.

WAR in the fifth domain. Are the mouse and keyboard the new weapons of conflict? ***The Economist***, Londres, 3. ed.,p. 25-28, 2010.