ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP INF MARTON DE ALMEIDA RAMOS

O CONTROLE DO CIBERESPAÇO PARA A MANUTENÇÃO DA SOBERANIA NACIONAL

Rio de Janeiro
2019

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP INF MARTON DE ALMEIDA RAMOS

O CONTROLE DO CIBERESPAÇO PARA A MANUTENÇÃO DA SOBERANIA NACIONAL

Trabalho Acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Defesa Cibernética.

Rio de Janeiro
2019

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

DIVISÃO DE ENSINO / SEÇÃO DE PÓS-GRADUAÇÃO

FOLHA DE APROVAÇÃO

Autor: **Cap Inf MARTON DE ALMEIDA RAMOS**

Título: **O CONTROLE DO CIBERESPAÇO PARA A MANUTENÇÃO DA SOBERANIA NACIONAL**

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

APROVADO EM _____/_____/_____ CONCEITO: _____

BANCA EXAMINADORA

Membro	Menção Atribuída
_____ **JOBEL SANSEVERINO JUNIOR - Maj** Cmt Curso e Presidente da Comissão	
_____ **EVERTON CAMPOS PINHEIRO - Cap** 1º Membro	
_____ **DEREK RODON BRASIL - Cap** 2º Membro e Orientador	
_____ **MARTON DE ALMEIDA RAMOS – Cap** Aluno	

O CONTROLE DO CIBERESPAÇO PARA A MANUTENÇÃO DA SOBERANIA NACIONAL

Marton de Almeida Ramos

Éverton Campos Pinheiro

RESUMO

Na era da informação e da grande evolução tecnológica que vive a sociedade atual, praticamente todos os serviços, indústrias, informações restritas dos governos federais são informatizadas e protegidas por algum sistema contra fraudes e invasões de terceiros. Nesse cenário analisamos a importância de um Estado soberano ser capaz de se proteger contra possíveis invasões desses vetores, que atuam silenciosamente no espectro eletromagnético desenvolvendo diuturnamente técnicas capaz de quebrarem os sistemas mais seguros do mundo. Nos anos 1990 e início dos anos 2000 existiram alguns cyber ataques a grandes multinacionais e poderosos Estados do cenário mundial, causando prejuízo de alguns bilhões de dólares para os afetados. O Brasil prevê em sua estratégia nacional de defesa o desenvolvimento de setores voltados aos estudos da segurança dos sistemas informatizados, para tanto a Força Terrestre inaugurou recentemente a Escola Nacional de Defesa Cibernética, voltada para as capacitações, pesquisas, desenvolvimento, operação e gestão de Defesa Cibernética com intuito de qualificar melhor a mão de obra para esse novo setor.

Palavras-chave: Defesa. Cibernética. Força Terrestre.

ABSTRACT

In the information age and the great technological evolution that live the current society, practically all the services, industries, and restricted information of the federal governments are computerized and protected by some system against fraud and invasions of weird people. In this scenario, we analyze the importance of a sovereign state be able to protect itself against possible invasions of these vectors, which act silently on the electromagnetic spectrum by day and night developing techniques that can break the safest systems in the world. In the 1990s and early 2000s there were some cyber attacks on grand multinationals and powerful states on the world stage, causing damage of a few billions dollars to those affected. Brazil foresees in its national defense strategy the development of sectors focused on studies of the security of computerized systems, for which the Army recently inaugurated the National School of Cyber Defense, focused on training, research, development, operation and management of Defense Cybernetics in order to better qualify the manpower for this new sector.

Key words: Defense. Cybernetics. Army.

[*] Capitão da Arma de Infantaria. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2010.

[**] Capitão da Arma de Infantaria. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2006. Pós graduado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO) em 2015.

1. INTRODUÇÃO

A revolução tecnológica alçou o espaço cibernético a uma nova condição nos assuntos relacionados à defesa e segurança. Tal espaço se caracteriza por um domínio global diante da dimensão informacional do ambiente operacional que consiste em uma rede interdependente de infra-estruturas de Tecnologia da Informação e Comunicações (TIC) e de dados, incluindo a internet, redes de telecomunicações, sistemas de computador, processadores embarcados e controladores.

O Brasil, como nação soberana, deve possuir aptidão para se proteger e contra-atracar às possíveis ameaças externas de forma geral, de modo compatível com suas utilidades e ambições político-estratégicas no cenário internacional. Isso possibilita ao país a consecução de objetivos estratégicos e a preservação dos interesses da nação, além do exercício do direito de defesa assegurado pela Constituição Federal.

No cenário mundial moderno, que tem como características marcantes a incerteza, volatilidade e evolução constante de possíveis ameaças ocultas, bem como pela presença de novos atores, agora não somente o Estado, nos possíveis cenários de conflito, a sociedade brasileira, em particular a expressão militar do Poder Nacional, deverá estar preparada de forma perene, sempre evoluindo, considerando os atuais e futuros litígios internacionais. Para tanto, medidas deverão ser escolhidas de forma a capacitá-la a responder oportunamente, antecipando os possíveis cenários desfavoráveis à Defesa e Soberania Nacional.

Intensificando ainda esse quadro, observa-se o aumento do risco de execução de ataques por Estados, organizações criminosas e até mesmo pequenos grupos, com as mais diversas motivações. Dentro desse cenário, a defesa do ciberespaço vem ganhando força, se estabelecendo como atividade fundamental ao êxito das operações militares, na medida em que assegura o exercício do Comando e Controle, função de combate essencial as operações militares, por meio da proteção dos ativos de informação, ao mesmo tempo permitindo que esse ativo seja negado ao agente opositor. A atividade cibernética, tem sua execução baseada em uma concepção sistêmica, com métodos, procedimentos, características e vocabulário peculiares, pois é tratada como uma atividade especializada, segundo o manual de Doutrina Militar e Defesa Cibernética.

1.1 PROBLEMA

É no cenário acima descrito, pois, que emerge a problemática da pesquisa que ora se delineia. Quais são os riscos que a vulnerabilidade do espaço cibernético, refletem para a soberania nacional?

Sob esse contexto a importância da pesquisa será decorrente de alguns casos históricos em que houve invasão de softwares de grandes potências mundiais, trazendo esses fatos para a realidade nacional, sobre as possíveis consequências que ações semelhantes acarretariam ao país.

Foram realizadas consultas na Constituição Federal, nos manuais do Ministério da Defesa, do Exército Brasileiro e do Exército dos Estados Unidos da América, e o caderno sobre a Política Nacional de Defesa e da Estratégia Nacional de Defesa. Foram consultados ainda, reportagens de casos históricos a cerca do assunto. A rede mundial de computadores foi amplamente utilizada como ferramenta de busca de dados.

O assunto controle do espaço cibernético atrelado a soberania nacional é visto como essencial, segundo o caderno sobre a Política Nacional de Defesa e da Estratégia Nacional de Defesa.

> Para que o desenvolvimento e a autonomia nacionais sejam alcançados é essencial o domínio crescentemente autônomo de tecnologias sensíveis, principalmente nos estratégicos setores espacial, cibernético e nuclear(BRASIL, 2012, p.19)

A partir do momento que setor cibernético alçou maior espaço no setor de segurança e soberania nacionais, ele foi divido em 02 partes: a primeira que é a segurança cibernética sob responsabilidade da Presidência da República e a segunda é a defesa cibernética controlada pelo Ministério da Defesa. O gráfico a seguir simplifica bem como são dividas as responsabilidades sobre o setor cibernético no país quanto aos níveis de decisão (Figura 1).

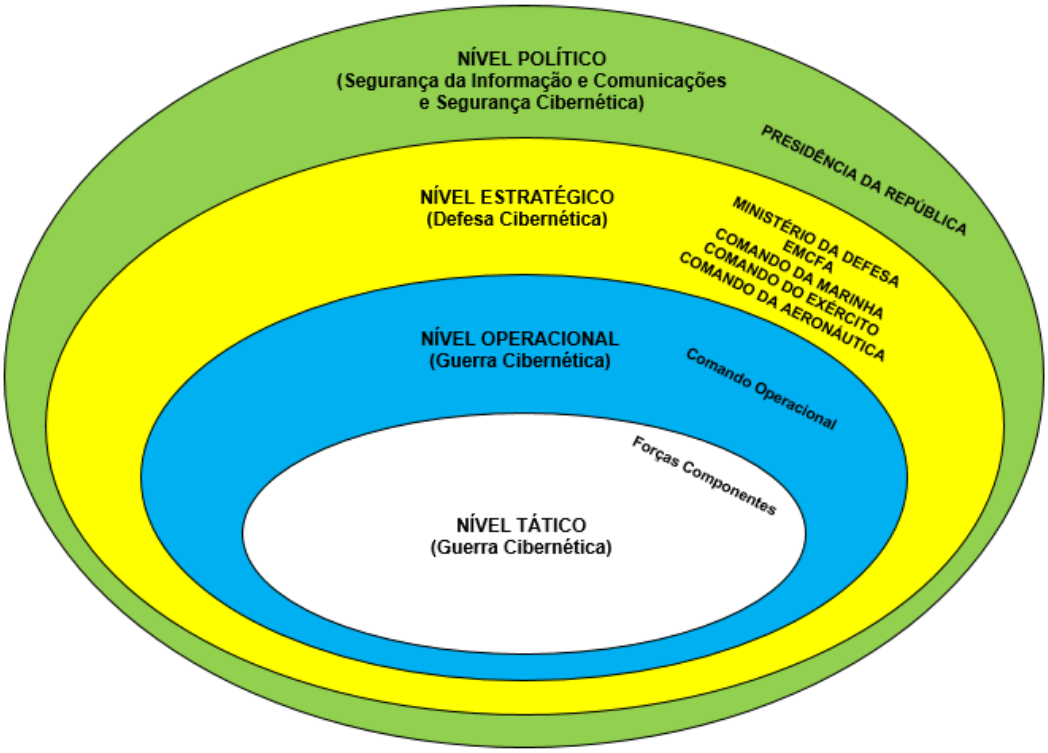

FIGURA 1 - Apresenta os níveis de decisão e respectivos responsáveis
Fonte:BRASIL, 2014, p.1-3

Dessa maneira o presente artigo tem por finalidade apresentar, por meio de pesquisa bibliográfica e documental, os possíveis problemas que um descaso com a defesa cibernética poderia acarretar ao país, a importância de se controlar o ciberespaço e como o Estado enxerga o presente assunto?

1.2 OBJETIVOS

A fim de consubstanciar a problemática cibernética, o presente estudo pretende apresentar a importância do controle do ciberespaço para manutenção da soberania nacional.

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

a) Apresentar aspectos da Política Nacional de Defesa e da Estratégia Nacional de Defesa, refletindo a visão atual do Estado quando da importância e relevância do assunto;

b) Apresentar a dimensão do campo cibernético, e como sua invasão ou descontrole podem ser nocivos a grandes nações;

c) Apresentar a estrutura/ capacidade gerais de proteção cibernética das forças armadas, especificamente do Exército Brasileiro.

1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

A presente pesquisa se justifica em virtude de o mundo está atravessando a era da informação, tendo no campo cibernético seu principal eixo de propagação e busca, pois a grande massa populacional se integra utilizando as tecnologias ligadas a cibernética.

A volatilidade com que os produtos ligados ao setor cibernético são criados, desenvolvidos ou aperfeiçoados nos leva a relembrar de forma análoga a corrida armamentista protagonizada pelos Estados Unidos e União Soviética durante a Guerra Fria na segunda metade do século XX, porém hoje essa corrida é disputada por grandes empresas multinacionais detentoras das tecnologias a fim de dominarem o mercado.

Tendo em vista de se minimizarem e evitarem possíveis problemas nas áreas informacionais e de segurança ligadas ao ciberespaço, foi criado o centro cibernético em Brasília, a fim de desenvolver a doutrina para mitigar possíveis ameaças nesse setor.

Para se opor a possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou permitam seu pronto restabelecimento (BRASIL, 2012).

Desse modo, enfatiza-se que o problema cibernético levantado poderá trazer benefícios para a Nação Brasileira, uma vez que os dispositivos tecnológicos sejam constantemente aperfeiçoados e suas vulnerabilidades sejam sanadas.

2. METODOLOGIA

A metodologia utilizada para busca de informações que justifiquem o estudo da problemática levantada, foi a pesquisa em livros, periódicos, artigos, projetos relacionados ao tema. Com o intuito de fazer um link de casos históricos com a possível ameaça que um sistema cibernético vulnerável está sujeito.

Com a pesquisa documental e qualitativa, para criar um vínculo entre o discurso teórico e a realidade apresentada, buscou-se analisar os fatos mais

relevantes que pudessem estar propícios de acontecer no território nacional convencendo o leitor da importância e sensibilidade do assunto.

2.1 REVISÃO DA LITERATURA

Iniciamos o delineamento da pesquisa com arcabouço histórico acerca dos casos mais conhecidos e relevantes dos últimos 30 anos, sendo baseada em uma revisão da literatura no período de 1994 a 2017. Essa delimitação baseou-se na necessidade de atualização do tema, visto que anterior a esse período as tecnologias voltadas ao mundo cibernético eram pouco desenvolvidas.

O limite anterior foi determinado almejando incluir as análises sobre eventos de invasões hackers em sistemas do Estado Norte Americano, bem como em alterações de softwares causando prejuízos milionários em empresas e bancos multinacionais, e mais recentemente a com a disseminação de vírus em sistemas específicos, causando grande prejuízo e tensão aos países atingidos, transformando essa nova forma de invasão, sem fins lucrativos, em terrorismo cibernético.

Foram utilizadas palavras chave como defesa, cibernética, força terrestre, hacker e vulnerabilidade, juntamente com seus correlatos em inglês, na busca de informações em manuais militares brasileiros e norte-americanos em sítios eletrônicos de procura na internet. O sistema de busca foi complementado pela coleta de informações em documentos como o Plano Nacional de Defesa e Estratégia Nacional de Defesa e a Constituição Federal de 1988.

2.2 COLETA DE DADOS

Voltando nossos olhares para o passado, mais precisamente entre fevereiro de 2001 e março de 2002, foi orquestrado, por um hacker escocês chamado Gary McKinnon, "o maior ato de pirataria de informática de todos os tempos" segundo o promotor do Estado da Virgínia (EUA), Paul McNulty. Gary McKinnon acessou ilegalmente e danificou mais de 57.000 computadores do exército americano, da aeronáutica, do pentágono e da Agência Espacial Americana (NASA). Fruto desse ato ilegal, McKinnon foi perseguido por 59 estados americanos e acusado de ter roubado informações que seriam úteis a possíveis inimigos do Estado Americano, além de ter causado um prejuízo de mais de 1 milhão de dólares aos cofres americanos. Segundo o próprio Gary McKinnon, as autoridades americanas se enganaram sobre os reais motivos de sua invasão, que era comprovar a existência

de OVNI e comprovar as falhas de segurança no sistema americano(KOUTROLARIS, 2018).

Um outro caso muito famoso, ocorrido no início dos anos 2000, foi o ataque a aos sites da Yahoo, Amazon e CNN por um hacker de 15 anos de idade, na época conhecido como "MafiaBoy". Esses ataques renderam um prejuízo de mais de 1,7 Bilhões de dólares para as empresas atacadas. Nos dias atuais, o canadense Michael Calce o "MafiaBoy" é especialista em segurança cibernética e alerta para as possíveis brechas nos sistemas informatizados que poderiam ser explorados por hackers, frisando que elo mais fraco do sistema são os operadores e é necessário maior atenção as impressoras, que são consideradas por ele portas de fácil acesso ao sistema de uma empresa(FOLHA DE SÃO PAULO, 2004).

Nos anos 1994, na hecatombe da era da internet, surgiu um jovem hacker russo chamado de Vladimir Lêvin, cuja história resume-se a invasão ao sistema de computadores do City Bank Of America (Citibank), um dos principais do setor bancário americano. Vladimir realizou inúmeras transferências das contas de grandes empresas para as contas de seus cúmplices espalhados pelo mundo, gerando um montante de US$10.700.952,00 de valores subtraídos das empresas. O hacker foi preso em Londres e cumpriu pena de três anos, se tornando o primeiro hacker russo cuja ação repercutiu em todo o mundo.(CIÊNCIA E TECNOLOGIA, 2017)

Os eventos mais recentes e sofisticados sobre forma de invasão de sistemas operacionais nacionais e/ou industriais ocorreu em meados de 2010, no que ficou conhecido como o vírus mais sofisticado do mundo, criado pelo grupo hacker *Equation Group* que possui ligação com o governo dos Estados Unidos. O caso ocorreu na Índia, Indonésia, porém teve mais notoriedade no Irã onde o vírus batizado de Stuxnet acessou as centrífugas de enriquecimento de urânio Iranianas que possuem o sistema operacional SCADA. Esse vírus tinha a capacidade de acessar, reprogramar as informações e esconder os rastros, e segundo Dimitry Bestuzhev analista regional da Kaspersky (empresa de soluções de segurança para a informática) "Um ataque como esse pode infectar milhares de máquinas no mundo todo, especialmente em países que trabalham com a tecnologia SCADA. O Stuxnet foi criado para sabotar ou restringir o funcionamento dessas infraestruturas", já Eugene Kaspersky que é Co-fundador e CEO da empresa definiu o episódio da seguinte maneira: "É aí que está a diferença e o marco para um novo mundo. A

década de 90 foi marcada pelos vândalos cibernéticos e os anos 2000 pelos cibercriminosos. Agora estamos entrando na década do terrorismo cibernético"(OLHAR DIGITAL, 2010).

Mais um advento interessante do mundo cibernético ocorreu em 2016, quando um grupo de cibercriminosos realizou um ataque DDoS (na linguagem da informática significa negação de serviço) considerado até então o maior já visto. Esse tipo de ataque cibernético consiste na utilização de gadgets, ou seja, uma porta alternativa como câmeras conectadas a internet, impressoras ligadas em rede, etc., para acessar as máquinas controladoras desses dispositivos, tudo com a finalidade de controlar o maior número possível de máquinas que por algum motivo possuísse algum tipo de ligação com a máquina principal. O alvo escolhido foi um blog "krebsonsecurity" mantido por um jornalista especilista em segurança da informação. Esse ataque permitiu aos criminosos controlarem milhares de máquinas, como se zumbis fossem(TECMUNDO, 2016).

Por fim mas não menos importante o caso mais famoso de um vírus, o wannacry. O wannacry é um ransomwarm, um tipo de calavo de tróia, porém com características de auto mutiplicação que rapidamente se espalha danificando máquinas e sistemas. De acordo com site Proof foram cerca de 345 mil máquinas infectadas em mais de 150 países tudo em um intervalo de 5 dias. O valor pelo resgate pedido não foi alto, U$300,00 por máquina pago em bitcoin, contudo o prejuízo global foi gigantesco, gerando uma insegurança em todas empresas do globo que utilizam o sistema operacional windows, o mais afetado no ataque(PROOF, 2017).

3. RESULTADOS E DISCUSSÃO

Analisando os casos históricos elencados neste artigo, conseguimos obter uma idéia geral de quão danoso pode ser um ataque cibernético para uma nação. A grande maioria dos casos de ataques de "crakers", como são conhecidos os hackers que utilizam os conhecimentos para gerarem o mal, ao longo da história foram a empresas, redes bancárias, contas particulares, visando auferir algum tipo de vantagem pecuniária. Outros casos foram para confrontar as empresas de segurança sobre quem possui maior habilidade no mundo cibernético ou simplesmente para roubar informações de Estado, causando o caos e gerando

enormes prejuízos a essas nações, podendo vir a ser a causa de conflitos entre nações.

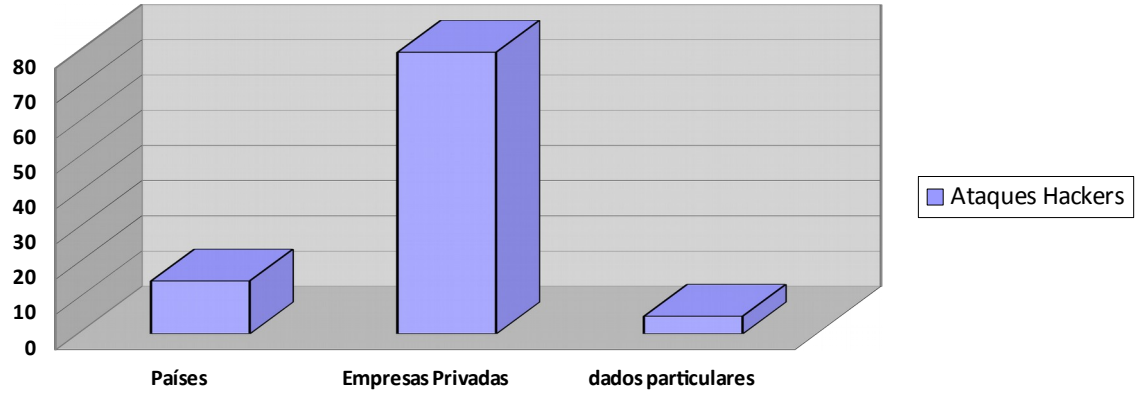

GRAFICO 1 - percentagem sobre a quantidade de ataque hackers e seus alvos nos últimos 30 anos.
Fonte: O autor

Olhando para o Estado brasileiro, observamos que estamos caminhando no sentido de mitigar as ameaças cibernéticas, tendo em vista o investimento das forças armadas como um todo no desenvolvimento de doutrinas, estabelecimento de centro de estudos nas áreas de cibernética, bem como o engajamento decisivo do Exército Brasileiro ao promover cursos nas áreas de guerra eletrônica e cibernética, no Centro de Instrução de Guerra Eletrônica (CIGE) em Brasília -DF. Esses ativos apóiam-se no modelo americano de enxergar a importância desse assunto para soberania nacional, segundo o manual de atividades cibernéticas e eletromagnéticas (EUA,2014):

> Devido à crescente dependência das capacidades ativadas pela rede, as operações terrestres unificadas são muito sensíveis às ameaças do ciberespaço e da guerra eletrônica, que podem comprometer a confidencialidade e a integridade da missão, sistema de comando e informações. Operações ofensivas inimigas no ciberespaço podem afetar as operações aliadas. A capacidade do adversário de acessar o ciberespaço do Exército pode resultar na manipulação de informações nos sistemas do Exército. Essa mudança pode influenciar futuras ações aliadas(por exemplo, atrasar ataque) e levar a uma redução da confiança nos sistemas aliados. A redução da confiança resulta em uma degradação da compreensão situacional do ambiente de informação do Exército(EUA, 2014 p.1-4)

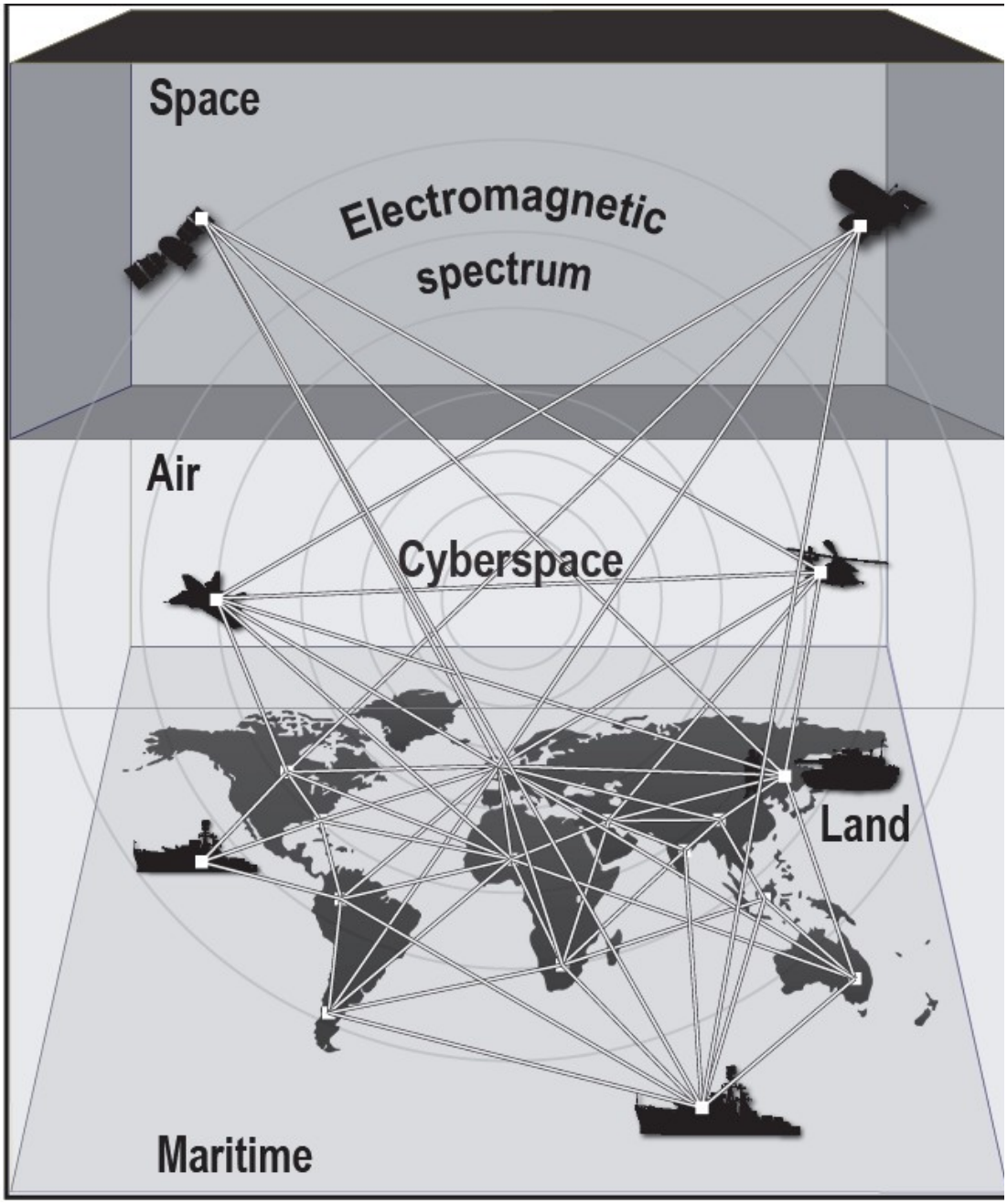

FIGURA 2 - Apresenta a abrangência e atividades cibernéticas e tudo que ela engloba
Fonte:EUA, 2014, p.1-4

4.CONSIDERAÇÕES FINAIS

A problemática da vulnerabilidade do espaço cibernético da nação brasileira ficou mais latente enquanto este artigo estava sendo produzido, no que diz respeito à segurança da informação, quando um site chamado "the intercept" cujo o proprietário possui ideologia esquerdista, invadiu o espaço cibernético particular de mensagens por aplicativos do Ministro da Justiça Sérgio Moro, modificando algumas

mensagens e divulgando na mídia de forma a denegrir o atual governo, atacando um dos símbolos de combate a corrupção no Brasil que é a Operação Lava Jato.

Este exemplo do parágrafo anterior somado aos ocorridos na década passada e década de 90, corroboram a importância do investimento e desenvolvido diuturno de novas tecnologias para combater ilícitos do ciberespaço. Nesse mundo cibernético sem lei, onde muitos vagam nas sombras com codinomes falsos e endereços irrastreáveis apenas buscando um brecha ou vulnerabilidade de um grande sistema, seja ele público ou privado, buscando tirar vantagens ilícitas para proveito próprio ou por meras motivações ideológicas, conseguimos entender da necessidade da busca de um escudo cada vez mais resistente contra um inimigo invisível com poder ataque muitas vezes desconhecido.

Nesse contexto, onde a principais batalhas são travadas do campo da informação sob o espaço cibernético, onde a disputa pela narrativa dominante é mais importante do que a verdade, essa batalha silente do ciberespaço requer uma força terrestre apta e moderna para contrapor quaisquer adversários que possa existir, segundo a estratégia nacional de defesa a responsabilidade do desenvolvimento de tecnologias cibernéticas é do Exército, e este aparenta estar se preparando e evoluindo muito neste setor tão sensível e caro para a soberania nacional.

REFERÊNCIAS

BRASIL, SENADO FEDERAL, SECRETARIA DE EDITORAÇÃO E PUBLICAÇÕES. **Constituição da República Federativa do Brasil 1988,** Brasília 2016.

_____, MINISTÉRIO DA DEFESA, EXÉRCITO, ESTADO-MAIOR. **Manual de Campanha Guerra Cibernética**. Estado Maior do Exército, 1ª Edição, 2017.

_____, MINISTÉRIO DA DEFESA, ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS, **Manual de Doutrina Militar de Defesa Cibernética**, 1ª Edição 2014.

_____, MINISTÉRIO DA DEFESA, EXÉRCITO, ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS, **Nota de Aula do Curso de Comunicações**, 1ª Edição 2019.

_____, MINISTÉRIO DA DEFESA, **Política Nacional de Defesa e Estratégia Nacional de Defesa**, Brasília 2012.

USA. Department of the Army,FM3-12, **Cyberspace and Electronic Warfare Operations**. Washington, DC, 2017.

_____. Department of the Army. FM3-38: **Cyber Electromagnetic Activities**. Washington, DC, 2014.

Koutroularis, **O Universo Desconhecido, A Verdade Sempre Esteve lá Fora.** Disponível em : https://koutroularis.wordpress.com/2018/03/27/gary-mckinnon/

Folha de São Paulo, **Hackers Canadá detém primeiro suspeito do maior ataque contra a rede de computadores, ocorrido em fevereiro**. Disponível em: https://www1.folha.uol.com.br/fsp/mundo/ft2004200011.htm

Olhar Digital, **Stuxnet: o vírus mais sofisticado que já existiu.** Disponível em: https://olhardigital.com.br/noticia/stuxnet-o-virus-mais-sofisticado-que-ja-existiu/14204

TecMundo**, Sim, você já pode usar o app que causou o maior ataque DDoS da história.** Disponível em**:** https://www.tecmundo.com.br/ataque-hacker/110431-sim-voce-usar-app-causou-o-maior-ataque-ddos-historia-mirai-hacker.htm

NakedSecurity, **Mirai "internet das coisas" malware de um ataque DDoS Krebs vai open source**. Disponível em: https://nakedsecurity.sophos.com/pt/2016/10/05/mirai-internet-of-things-malware-from-krebs-ddos-attack-goes-open-source/

Proof, **WannaCry: o primeiro ransomworm na indústria de cibersegurança**. Disponível em: https://www.proof.com.br/blog/wannacry-ransomworm/

Proof, **Todo ataque tem uma história: entenda o contexto do *WannaCry* e porque ele é *pop***. *Disponível em:* https://www.proof.com.br/blog/contexto-do-wannacry/

ANEXO A - SOLUÇÃO PRÁTICA

O estudo do tema aborda basicamente os perigos que um ciberespaço vulnerável pode acarretar para a soberania nacional, porém essa temática leva o leitor a refletir sobre os problemas em um nível macro, conhecendo problemas mundiais com consequências políticas. Como já abordado no trabalho, não é possível viver conectado a nível mundial sem a integração cibernética, e é nesse vasto universo invisível onde estão a maioria se não a totalidade das informações mundiais relevantes.

Como fruto do resultado obtido com a pesquisa, puxando para ótica da Força Terrestre, que é a responsável pelo desenvolvimento do sistema de defesa cibernética previsto na Estratégia Nacional de Defesa, deve-se voltar a atenção por mais simples que seja para as condições atuais dos sistemas informacionais utilizados pelo Exército e sua confiabilidade quanto a segurança cibernética.

O Exército Brasileiro, possui inúmeros sitios ligados diretamente a Internet e alguns softwares ligados indiretamente a grande rede, como os sitemas Sped, Siscofis, conduzidos pela intranet, porém com uma grande avenida desprotegida que é sua ligação a internet por meio de portas VPN.

O manual EB70-MC-10.232 Guerra Cibernética aborda de maneira sucinta os fundamentos, perigos e forma de utilização do setor cibernético nas operações, todavia seria interessante uma nota doutrinária que abordasse a necessidade da segurança cibernética nas atividades diárias das OM, capacitando os recursos humanos para mitigarem possíveis vulnerabilidades nos sistemas.