ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP QMB MARLON ANDERSON SANTIAGO DAFLON

MODELOS DE DOMINAÇÃO DO ESPAÇO CIBERNÉTICO:

AS ABORDAGENS BRASILEIRA E RUSSA À GUERRA CIBERNÉTICA

Rio de Janeiro

2020

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP QMB MARLON ANDERSON SANTIAGO DAFLON

MODELOS DE DOMINAÇÃO DO ESPAÇO CIBERNÉTICO:

AS ABORDAGENS BRASILEIRA E RUSSA À GUERRA CIBERNÉTICA

Artigo Científico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito parcial para a obtenção da pós-graduação Lato Sensu em Ciências Militares.
Orientador: Cap Guilherme Polidori Cabral.

Rio de Janeiro

2020

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 QMB MARLON ANDERSON SANTIAGO DAFLON

Título: **MODELOS DE DOMINAÇÃO DO ESPAÇO CIBERNÉTICO:**
AS ABORDAGENS BRASILEIRA E RUSSA À GUERRA CIBERNÉTICA

Artigo Científico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito parcial para a obtenção da pós-graduação Lato Sensu em Ciências Militares.

APROVADO EM _____/_____/_____ CONCEITO: _____

BANCA EXAMINADORA

Membro	Menção Atribuída
_____ **EMERSON RODRIGUES DA SILVA - TC** Cmt C Log e Presidente da Comissão	
_____ **GUILHERME POLIDORI CABRAL - Cap** 1º Membro/Orientador	
_____ **LUIZ FERNANDO GOMES RAMOS - Cap** 2º Membro	

_____
MARLON ANDERSON SANTIAGO DAFLON – Cap
Aluno

MODELOS DE DOMINAÇÃO DO ESPAÇO CIBERNÉTICO: AS ABORDAGENS BRASILEIRA E RUSSA À GUERRA CIBERNÉTICA

Marlon Anderson Santiago Daflon[1]

Guilherme Polidori Cabral[2]

RESUMO

Um importante alicerce que estrutura os conflitos militares modernos é a implementação prévia de medidas de guerra cibernética. O combate cibernético favorece os objetivos estratégicos e políticos sem a utilização da força militar convencional e, por consequência, molda uma resposta favorável da comunidade da imprensa, eis que a utilização da força militar convencional no teatro de operações apresenta-se postergada ou reduzida em detrimento do combate informacional. Sob este raciocínio, é imperioso destacar que os instrumentos da guerra cibernética são comumente utilizados antes do início das operações militares e se situam sob dois importantes aspectos: inicialmente, para alcançar os objetivos estratégicos do Estado sem a utilização da força e, quando necessários, para desorientar e desinformar chefes de governo, desmoralizar as ações do adversário, organizar protestos antigoverno ou influenciar a opinião pública. Assim, a guerra cibernética pode representar uma prática hodierna de um Estado em tempos de paz, com vistas a controlar potências mundiais, sem, contudo, afrontar-lhes a soberania territorial propriamente dita, representando, portanto, uma ferramenta legítima de postergação do combate cinético.

Palavras-chaves: Ciberespaço; Poder cibernético, Internet, Infraestrutura, Rússia, Políticas cibernéticas; Cyberwarfare; Relações cibernéticas internacionais.

ABSTRACT

An important foundation that structures modern military conflicts is the prior implementation of cyber warfare measures. Cyber combat favors strategic and political objectives without the use of conventional military force and, consequently, shapes a favorable response from the press community, since the use of conventional military force in the theater of operations is postponed or reduced to the detriment informational combat. Under this reasoning, it is imperative to point out that the instruments of cyber warfare are commonly used before the beginning of military operations and are located under two important aspects: initially, to achieve the strategic objectives of the State without the use of force and, when necessary, to disorient and misinform heads of government, demoralize the opponent's actions, organize anti-government protests or influence public opinion. Thus, cyber war can represent a current practice of a State in times of peace, with a view to controlling world powers, without, however, confronting the territorial sovereignty itself, representing, therefore, a legitimate tool for postponing the kinetic combat.

Keywords: Cyberspace; Cyber power, Internet, Infrastructure, Russia, Cyber policies; Cyberwarfare; International cybernetic relations.

---

[1]Capitão do Quadro de Material Bélico. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2011.

[2]Capitão do Quadro de Material Bélico. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2008. Pós-graduado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (ESAO) em 2018.

1. INTRODUÇÃO

A compreensão do comportamento do adversário no domínio cibernético é um desafio. As decisões relativas à invasão de sites governamentais estrangeiros, a extração de informações estratégicas de defesa nacional e, sobretudo, o tratamento dessas informações pelo País invasor, revelam a face obscura e devastadora de uma guerra em que o campo de batalha pode ocorrer tranquilamente numa sala por meio de um computador.

Em contrapartida, os desafios conceituais associados à ciber-guerra demonstram que as ameaças tecnológicas se desenvolvem de forma tão intensa, que é impossível enquadrar a guerra cibernética em conceitos estáticos ou analisá-la sob uma perspectiva puramente tática e defensiva.

Sendo assim, em que pese a relativa falta de conhecimento do potencial cibernético do inimigo, equiparar nossos conhecimentos digitais ao de alguns países seria uma falha estratégica sem precedentes, uma vez que esta área de conhecimento se encontra em constante desenvolvimento e os ciberataques são o principal meio para o real conhecimento do potencial cibernético do inimigo.

1.1 PROBLEMA

Muito embora a internet não tenha sido criada com aspirações militares tampouco com o objetivo de interferir nas infraestruturas estratégicas de outros países, no século XXI, uma nação que não possui as competências necessárias para proteger seu espaço cibernético torna-se muito vulnerável.

Os sistemas cibernéticos possibilitam a gestão de toda a infraestrutura de uma nação, indo desde seu sistema satelital de análise meteorológica até o tratamento e distribuição de água, por exemplo.

Mas as vantagens proporcionadas pelos sistemas cibernéticos com a automação e a informatização dos sistemas de controle vêm acompanhadas de

vulnerabilidades que exigem um eficiente sistema de defesa para garantir o uso do espaço cibernético com certa margem de segurança.

Importante destacar desde o início que, quando se trata de ambiente cibernético, não existe lugar completamente seguro. Sob esse raciocínio e de forma bem introdutória, tem-se que a exploração das vulnerabilidades nos sistemas informatizados dos oponentes constitui uma das ferramentas da guerra cibernética.

Sendo assim, a guerra cibernética se revela em uma nova dimensão no campo de batalha moderno que pode trazer enorme vantagem quando bem empregada por um dos beligerantes ou negligenciada pelo outro.

Diante desse cenário, em que o campo de batalha virtual ganha cada vez mais importância, seria possível dominá-lo, sabotando os sistemas do inimigo e garantindo ao próprio país o uso totalmente seguro desse espaço? Ou então seria possível controlar o uso do espaço cibernético por civis, evitando a utilização do meio cibernético para o cometimento de crimes patrimoniais, à imagem ou até mesmo ações terroristas?

1.2 OBJETIVOS

Os objetivos da investigação a ser realizada podem ser assim descritos:

1.2.1 OBJETIVO GERAL

O objetivo geral é verificar se é possível dominar o espaço cibernético analisando modelos de controle exercidos pelo Brasil e pela Rússia.

1.2.2 OBJETIVOS ESPECÍFICOS

Serão observados os seguintes objetivos específicos:

a) Analisar as características da gestão e do controle do espaço cibernético executado no Brasil a luz das diversas legislações sobre o tema.

b) Analisar as características da gestão e do controle do espaço cibernético executado na Rússia a luz de documentos e artigos desenvolvidos sobre o tema, bem como de episódios históricos.

c) Estabelecer uma comparação entre os modelos brasileiro e russo visando avaliar o que as competências cibernéticas russas teriam a contribuir com o desenvolvimento cibernético brasileiro.

1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

O controle do espaço cibernético garante a uma nação a proteção de seus ativos de infraestrutura e de combate bem como a possibilidade de interferir nos sistemas do oponente, podendo causar uma infinidade de danos, como por exemplo, a inserção de um vírus que seja capaz de apagar um banco de dados governamental ou interferir no funcionamento de uma usina nuclear, podendo gerar consequências catastróficas.

A história recente é capaz de contar como ataques cibernéticos podem influenciar os sistemas de defesa nacionais, a saber:

- Ciberataques à Estonia, em 2007, que deixou sites do governo fora de funcionamento por dias;
- Conflito entre Rússia e Geórgia, em 2008;
- Conflito entre Rússia e Ucrânia: ataque cibernético à rede de energia elétrica em 2015.
- Célula terrorista nos Jogos Olímpicos do Rio de Janeiro, em 2016.

É por esse potencial destrutivo que o domínio do ambiente cibernético é extremamente necessário a qualquer força militar. Seja para sua defesa, evitando um ataque, por exemplo, seja para utilização como forma de ataque, degradando os sistemas de informação do oponente ou ainda como forma de monitoramento das

atividades cibernéticas de outro país, por meio da análise de dados sigilosos de interesse mundial e que se encontram em posse dessa Nação.

2. REVISÃO DE LITERATURA

O estudo das técnicas de guerra cibernética nos conflitos militares modernos possui vasta literatura no âmbito do Direito Público Internacional. Ademais, sua aplicação é verificada em todas as estruturas governamentais em nível estratégico. Desta forma, para aprofundar o tema da guerra cibernética nos conflitos militares modernos, buscou-se realizar uma pesquisa a ramos diversificados, desde manuais militares à legislação de direito público interno.

No fito de contextualizar todo o material objeto de consulta, serão apresentados fatos históricos atinentes ao tema.

Ressalta-se que não compunha o objeto de estudo as diversas técnicas de "guerra da informação". Vale lembrar que o referido tema é muito mais abrangente e comporta diversas abordagens, sendo a guerra cibernética um dos meios para se realizar guerra da informação. Sendo assim, os dois termos não se confundem e representam dimensões diferentes do combate, podendo ou não ser utilizadas em conjunto.

Sendo assim, a fim de nortear a pesquisa, as palavras-chave utilizadas foram: o Sistema de Defesa Cibernética Brasileiro; o Sistema Cibernético Russo; Poder cibernético; Internet; Infraestrutura; Rússia; Políticas cibernéticas; Cyberwarfare; Relações cibernéticas internacionais.

a. Critérios de inclusão:

- Legislação, documentos, manuais e publicações sobre os aspectos da guerra cibernética nos conflitos militares modernos.

- Publicações sobre os aspectos da doutrina militar russa relativos à guerra cibernética, bem como citações constantes em documentos.

b. Critérios de exclusão:

- Estudos que tratam da guerra informacional em sentido amplo não especificando a técnica abordada, pois fogem do campo de estudo pretendido.

3. METODOLOGIA

O levantamento das competências cibernéticas brasileiras será avaliado por meio do Manual de Campanha de Guerra Cibernética, pela Política Nacional de Defesa e pela Estratégia Nacional de Defesa.

O levantamento das competências cibernéticas da Rússia será analisado a luz de artigos e trabalhos monográficos realizados para estudar as ações do governo russo no ambiente virtual, livros publicados em língua inglesa que tratam do tema *cyberwar*, bem como a partir de matérias veiculadas em sites internacionais ou especializados.

De posse desse material será realizada uma pesquisa descritiva para se atingir os objetivos gerais e específicos propostos.

4. RESULTADOS E DISCUSSÕES

Conforme a metodologia descrita no capítulo anterior, seguem os resultados encontrados na pesquisa documental bem como nas discussões sobre o tema.

4.1. PESQUISA DOCUMENTAL

De modo a facilitar a compreensão do tema escolhido, os resultados da pesquisa documental foram separados em subtópicos.

4.1.1 DEFINIÇÕES

Para definir o espaço cibernético, apresento as considerações expostas por Pierre Lévy, mestre em História da Ciência e pesquisador reconhecido nas áreas da cibernética, inteligência artificial e internet, em seu livro Cibercultura:

> É o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo (LÉVY, 1999. p. 17)

Numa definição mais simplista ciberguerra ou guerra cibernética, encontrada na Wikipedia, é a "modalidade de guerra onde a conflitualidade não ocorre com armas físicas, mas através da confrontação com meios eletrônicos e informáticos no chamado ciberespaço." (CIBERGUERRA, 2020)

Sob a perspectiva governamental, define-se Segurança Cibernética nos termos da Portaria GSIPR nº 45, do Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, publicada no DOU de 09 de setembro de 2009:

> Arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas (BRASIL, 2009).

No Manual de Campanha de Guerra Cibernética, o termo Guerra Cibernética define-se como:

> Uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C2 ao adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de TIC(tecnologia da informação e comunicação) para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sistemas de Informação. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação às TIC (BRASIL, 2017).

4.1.2 AMBIENTE DE ATUAÇÃO DA GUERRA CIBERNÉTICA SOB A ÓTICA BRASILEIRA – ATUAÇÃO CIVIL

Em 4 de junho de 2014, a Polícia Federal inaugurou o Centro de Monitoramento do Serviço de Repressão a Crimes Cibernéticos em Brasília. Conforme manifestação do Órgão:

> As mais de 320 redes do Governo Federal recebem mais de dois mil ataques por hora e o objetivo do centro inaugurado será identificar e acompanhar, continuamente, os responsáveis por estes ataques, permitindo uma ação mais rápida e eficaz. Evita-se, com isto, maiores danos aos sistemas ou aos dados sensíveis do governo ou dos cidadãos brasileiros (BRASIL, 2012).

A iniciativa da Polícia Federal ocorreu quando os principais episódios mundiais de ciberataques já haviam sido deflagrados, sobretudo na Rússia e nos Estados Unidos da América. Nesse raciocínio, a criação do Centro de Monitoramento do Serviço de Repressão a Crimes Cibernéticos sinaliza a preocupação do Estado Brasileiro em coibir a prática cibernética criminosa.

Mais adiante, o Ministro de Estado da Justiça e Segurança Pública, no uso da atribuição que lhe confere o artigo 87, parágrafo único, inciso I, da Constituição Federal, publicou a Portaria nº 1.252, de 29 de dezembro de 2017, que aprova o Regimento Interno da Polícia Federal.

O referido regimento estabelece que o Serviço de Repressão a Crimes Cibernéticos – SRCC, passa a integrar a estrutura da Polícia Federal. Sendo assim, do ponto de vista operacional, os dados coletados em ambiente virtual com potencial criminoso passam a ser averiguados em departamento específico dentro da Polícia Federal, onde lhes é dispensado o devido tratamento.

Sob análise em nível estratégico, a Estrutura Regimental do Gabinete de Segurança Institucional da Presidência da República, aprovada pelo Decreto nº 9.668, de 2 de janeiro de 2019, estabelece que compete ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI) planejar, coordenar e supervisionar a atividade de segurança da informação no âmbito da administração pública federal, nela incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas, bem como manter o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, de responsabilidade nacional, para a proteção cibernética.

Por fim, é importante mencionar o Decreto nº 10.222, de 5 de fevereiro de 2020 que aprova a Estratégia Nacional de Segurança Cibernética - E-CIBER para o

quadriênio 2020-2023, e representa “orientação manifesta do Governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética”.

Os objetivos estratégicos do E-CIBER são:

1. Tornar o Brasil mais próspero e confiável no ambiente digital;

2. Aumentar a resiliência brasileira às ameaças cibernéticas; e

3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional.

Em que pese o amplo escopo de atuação, ao analisarmos as competências atribuídas à PF, ao GSI e à Presidência da República é possível verificar uma atuação eminentemente repressiva com especial ênfase à segurança do espaço cibernético.

Não se verifica, pelo menos de forma ostensiva, portanto, o viés ofensivo - característico do cenário de ciberguerra -, no rol de competências das Instituições Públicas Civis, eis que tal atuação, assim como qualquer outra ação de guerra, encontra-se delegada às Forças Armadas. No entanto, a capacidade desenvolvida pela Polícia Federal na repressão de ações no espaço cibernético, tornar-se uma importante competência em caso de guerra declarada, com o fito de realizar o monitoramento das atividades inimigas no ambiente virtual.

4.1.3 AMBIENTE DE ATUAÇÃO DA GUERRA CIBERNÉTICA SOB A ÓTICA BRASILEIRA – ATUAÇÃO MILITAR

A Estratégia Nacional de Defesa estabeleceu três setores para a Defesa Nacional: Nuclear, Espacial e Cibernético.

O referido documento prevê que o Ministério da Defesa e as Forças Armadas intensificarão as parcerias estratégicas nos três setores citados e deverão atuar em conjunto, com vistas à potencialização das defesas cibernética, nuclear e espacial. No entanto, cada Força recebeu atribuição de gerenciar um setor, cabendo ao Exército o processo de estruturação do Setor Cibernético.

Eis o teor da Estratégia Nacional de Defesa - END do Brasil, aprovada pela primeira vez em 18 de dezembro de 2008:

> No setor cibernético, o Ministério da Defesa e o Ministério da Ciência Tecnologia e Inovação, por intermédio do Departamento de Ciência e

> Tecnologia do Exército, promoverão ações que contemplem a multidisciplinaridade e a dualidade das aplicações; o fomento da Base Industrial de Defesa com duplo viés: aquisição de conhecimento e geração de empregos; e a proteção das infraestruturas estratégicas, com ênfase para o desenvolvimento de soluções nacionais inovadoras (BRASIL, 2008).

Após a apresentação da Estratégia Nacional de Defesa – END, o Ministério da Defesa criou o Programa da Defesa Cibernética na Defesa Nacional cujo principal objetivo é incrementar as atividades de capacitação, doutrina, ciência, tecnologia e inovação, inteligência e operações no âmbito da Defesa Nacional.

Importante ressaltar que o Programa da Defesa Cibernética na Defesa Nacional desenvolveu o Sistema de Homologação e Certificação de Produtos de Defesa Cibernética, através de termo de execução descentralizada entre o Inmetro e o Departamento de Ciência e Tecnologia do Exército que possibilitará a detecção de back doors, malwares e outras ameaças cibernéticas.

O Sistema de homologação e certificação de produtos de defesa cibernética trata-se de um programa de avaliação de riscos e conformidade. Nas palavras do Instituto Nacional de Metrologia, Qualidade e Tecnologia – Inmetro: “a ideia é desenvolver metodologias e ensaios para avaliação de ativos de tecnologia da informação e comunicação, como roteadores, switches, firewalls, softwares de e-mail, entre outros, a fim de mitigar a ocorrência de ataques cibernéticos.”

O ambiente de atuação da Guerra Cibernética no contexto das funções de combate é representado por três capacidades operativas, conforme Manual de Campanha de Guerra Ciberética:

a) Proteção cibernética
b) Ataque Cibernético
c) Exploração Cibernético

A articulação conjunta das três capacidades operativas, cada qual em sua especificidade de tarefa, orienta o ambiente de atuação de forma a neutralizar o ataque e a exploração cibernética do oponente.

Outro ponto a se destacar a respeito da Guerra Cibernética é o baixo investimento necessário para o emprego deste vetor de combate, quando comparado a um armamento de alta tecnologia, como uma Bateria de Foguetes Astros, por exemplo, que possui munições de elevado valor, sem mencionar o custo milionário do próprio armamento, além de toda a cadeia logística que o equipamento exige como manutenção, armazenamento e segurança.

Por outro lado, quando se trata de guerra cibernética, o maior investimento se aplica no desenvolvimento intelectual do combatente. Já a estrutura física computacional, uma vez implementada, possui baixo custo de manutenção.

Do gasto com investimento em potencial humano deve-se ainda ser deduzido o feedback positivo de tal investimento, uma vez que os benefícios do aprendizado se voltam para a própria instituição.

Pensando na capacitação como componente apto a enfrentar ameaças cibernéticas, o General Aderico Mattioli, atual Coordenador do Escritório Central do Sistema Defesa, Indústria e Academia de Inovação (SisDIA)**,** menciona o seguinte na Revista “em discussão! ” do Senado Federal:

> Deveríamos ter, no mínimo, a capacitação em bancos escolares, na educação, para formarmos também uma capacidade produtiva e o entendimento de produto de defesa, que não é mais aquele produto materializado propriamente dito. A cibernética, talvez, seja a mais vulnerável na nossa realidade e a mais exequível a curto prazo, a que demande menos recurso para darmos um grau de proteção — vamos chamar de firewall — mínimo necessário para o país. É uma área com a qual podemos contribuir muito (MATTIOLI, 2012).

Nessa linha de raciocínio, o ambiente de atuação da Guerra Cibernética, sob a perspectiva das competências militares, encontra-se em latente expansão através da celebração de acordos e estabelecimento de parcerias com diversos órgãos públicos, tudo no fito de intercambiar potencialidades de diferentes setores, uma vez que as competências a serem desenvolvidas pelo campo da cibernética são multidisciplinares e interdependentes.

E por fim, com objetivo de apresentar algumas linhas do arcabouço teórico acerca da atuação da Guerra Cibernética sob a ótica Brasileira, segundo o Manual de Campanha de Guerra Cibernética, as ações no espaço cibernético são compostas das seguintes denominações, de acordo com o nível de decisão a ser adotado:

a) nível político - Segurança da Informação e Comunicações (SIC) e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo a administração pública federal (APF) direta e indireta, bem como as infraestruturas críticas da informação inerentes às infraestruturas críticas nacionais;

b) nível estratégico - Defesa Cibernética - a cargo do MD, Estado-Maior Conjunto das Forças Armadas (EMCFA) e comandos das FA, interagindo com a Presidência da República e a APF; e

c) níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das FA.

Para ilustrar os níveis de decisão no que tange ao tratamento de ações no espaço cibernético, segue abaixo gráfico retirado do Manual de Campanha de Guerra Cibernética:

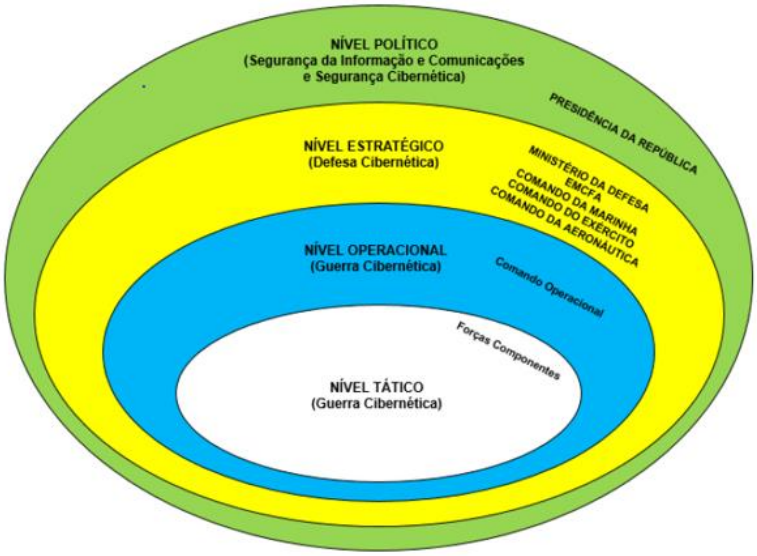

FIGURA 1 – Níveis de Decisão
Fonte: Manual de Campanha de Guerra Cibernética

4.1.4 AMBIENTE DE ATUAÇÃO DA GUERRA CIBERNÉTICA SOB A ÓTICA RUSSA.

A Rússia é precursora da tecnologia de guerra cibernética e já demonstrou ao longo da história recente que possui habilidades bem específicas capazes de desarticular diversas operações do inimigo, através da disseminação de vírus, warms e outras pragas virtuais.

O General Valery Gerasimov, atual Chefe das Forças Armadas Russas, em seu artigo, "O Valor da Ciência na Predição", menciona o seguinte:

> No século XXI, temos visto uma tendência a esbater as linhas entre os estados de guerra e de paz. As guerras já não são declaradas e, tendo começado, prosseguem de acordo com um modelo desconhecido. A experiência dos conflitos militares - incluindo aqueles ligados às chamadas revoluções coloridas no Norte de África e no Oriente Médio - confirma que um Estado perfeitamente próspero pode, em questão de meses e até dias, transformar-se em uma arena de conflito armado feroz, tornar-se vítima da intervenção estrangeira e afundar-se em uma teia de caos, catástrofe humanitária e guerra civil (GERASIMOV, 2016, p. 24).

Em alusão aos movimentos liberais do norte da África intitulados Primavera Árabe, o General Valery Gerasimov, ainda menciona:

> O espaço de informação abre amplas possibilidades assimétricas para reduzir o potencial de combate do inimigo. No Norte de África, assistimos ao uso de tecnologias para influenciar as estruturas estatais e a população com a ajuda de redes de informação (GERASIMOV, 2016, p.27).

Verifica-se, portanto, o estado latente e constante do alto comando militar russo no que tange à utilização de técnicas de Guerra Cibernética, seja em tempos de guerra ou em tempos de paz. Nesse sentido, de forma exemplificativa, serão abordados três momentos históricos que evidenciaram algumas das manobras cibernéticas adotadas pelos russos.

4.1.5. ESTÔNIA (2007): UM MARCO CIBERNÉTICO.

Acredita-se que os eventos de ciberataques à Estônia tenham ocorrido como retaliação à decisão do governo estoniano de mover uma estátua de bronze de um soldado soviético de um lugar central da cidade de Tallinn, capital da Estônia, para um cemitério militar localizado em local ermo fora do centro da cidade.

A referida estátua homenageava os soldados soviéticos-russos no episódio de libertação da Estônia da Alemanha nazista na Segunda Guerra Mundial.

A decisão do Governo Estoniano afrontou a Rússia, uma vez que ainda residiam em território Estoniano uma população de etnia russa, ainda que minoritária. Ademais, a retirada da estátua ocorreria, segundo o Governo russo, na véspera de um “feriado sagrado", referindo-se ao dia 9 de maio, dia que a Rússia celebra a vitória contra o fascismo da Alemanha Nazista.

A remoção da estátua ocorreu em 27 de abril de 2007, e desencadeou uma série de protestos de etnia russa na Estônia, resultando na prisão de aproximadamente 1.300 pessoas e algumas mortes.

A partir daí os primeiros ataques DDoS tiveram como alvo os sites do governo estoniano. Foram ao todo 3 ondas de ataques cibernéticos.

DDoS é um recurso conhecido como ataque de negação de serviço, cujo objetivo é tornar os recursos de um sistema indisponíveis devido à sobrecarga de informações enviadas.

Durante a primeira onda, os ataques DDoS sobrecarregaram os servidores dos sites do Parlamento, dos partidos políticos, dos maiores bancos do país, e dos veículos de notícias e telecomunicações do Estônia.

Em maio de 2007, os fornecedores de serviços de Internet (ISP) trabalharam em conjunto com as autoridades estonianas para bloquear dados maliciosos e defender as redes da Estónia. No entanto, a parceria não evitou a segunda onda de ataques mais sofisticada, que atingiu o país entre os dias 8 e 9 de maio de 2007.

Na segunda onda, os BOTNET`s (computadores-zumbis sequestrados em todo o mundo) congestionaram novamente os endereços da internet estoniana com dados errados, forçando-os a desligar. Aproximadamente 58 ataques BOTNET`s atingiram sites estonianos, somente nos dias 8 e 9 de maio.

Os ataques ocasionaram o encerramento das operações online do Banco Hansabank, o maior banco estoniano, e consequentemente, a não realização de diversos negócios financeiros.

Uma terceira onda de ataques ocorreu na semana seguinte. Desta vez, os hackers invadiram sites pessoais e postaram suas próprias mensagens.

Os ataques DDoS contra a Estônia durante os meses de abril e maio de 2007 constituem o primeiro uso coordenado da cibernética em grande escala pela Rússia para afetar um País.

As consequências dos ataques foram devastadoras. Os sites de internet da Estônia foram inundados por PING (Packet Internet Network Groper ou localizador de pacotes na rede de internet) e por dados de entupimento de rede, forçando a maioria dos sites, públicos ou privados, a encerrar suas conexões internacionais.

Desta forma, os ataques cibernéticos bloquearam grande parte da capacidade do país de se comunicar ou compartilhar informações com o mundo.

Importante ressaltar que em 2007, aproximadamente 60% dos 1,3 milhões de cidadãos estonianos já utilizavam a internet regularmente, o que representou significativa recessão, uma vez que os negócios estabelecidos pela internet sofreram

descontinuidade momentânea, sem mencionar a perda da confiabilidade das plataformas digitais.

Nesse sentido, Urmas Paet, Ministro dos Negócios Estrangeiros da Estônia à época, mencionou que "os ataques [eram] virtuais, psicológicos e reais".

Em verdade, a Rússia nunca reivindicou os ataques cibernéticos de 2007, no entanto, o apoio deliberado às ações dos hackers pôde determinar o posicionamento russo diante do episódio, bem como determinar o quão curta é a tolerância interventiva da Rússia a ponto de apoiar operações cibernéticas ofensivas capazes de desacreditar o governo estoniano e desestabilizar toda a rede informatizada do País, a partir de um estopim relativamente pequeno – a estátua de Tallinn.

No livro Malicious Bots, de Ken Dunham e Jim Melinick, consta citação do Ministro da Defesa Estoniano no período, Sr Jaak Aaviksoo:

> É verdade que o objetivo desses atacantes era desestabilizar a sociedade estoniana, criando ansiedade entre as pessoas de que nada está funcionando, os serviços não são operáveis, isso foi claramente um terror psicológico de certa forma (DUNHAM; MELINICK, 2008, p. 121).

Por fim, o chamado Soldado de Bronze, cujo deslocamento do centro da capital Tallinn tinha originalmente provocado o conflito entre Estônia e Rússia, permaneceu na sua nova localização, no Cemitério Militar, num lugar ermo na periferia da cidade, mas o posicionamento russo foi mostrado e não apenas os estonianos agora sabem o limite da tolerância russa.

Diante do episódio, é importante destacar que o impacto dos ataques alcançou um nível estratégico de metodologia e organização. As três ondas de ataques cibernéticos foram a primeira demonstração do *cyberwar* como meio de coerção não-interventiva na história.

O impacto ressoou no mundo de tal forma que a OTAN - Organização do Tratado do Atlântico Norte, criou o “Cooperative Cyber Defense Centre for Excellence” (CCDCOE), com sede em Tallinn – capital da Estônia.

O Centro de Excelência em Defesa Cibernética Cooperativa da OTAN é um centro multinacional e interdisciplinar de defesa cibernética que apoia os países membros e a OTAN no desenvolvimento de pesquisas e tecnologias voltadas ao fortalecimento da defesa cibernética.

4.1.6. RÚSSIA E GEÓRGIA (2008): AÇÃO COORDENADA MUNDIALMENTE.

A região da Ossetia do Sul corresponde a uma área de aproximadamente 3.900 km² e conta com diversas disputas territoriais entre os países da Rússia e da Geórgia.

Em agosto de 2008, a Rússia atacou a Geórgia em resposta à tentativa desse país de reincorporar a região da Ossetia do Sul.

A semelhança do episódio vivido pela Estônia, uma série de ataques DDoS congestionou os sites do país e derrubou as redes da Geórgia, cortando as comunicações dos bancos georgianos, das empresas e provedores privados de telecomunicações.

Desta vez, os ataques foram ainda mais organizados. Sites russos, como o www.stopgeorgia.ru, forneceram listas de sites georgianos e disponibilizaram ainda instruções com download de worms e outros malwares para facilitar o ataque. Por meio do anonimato, qualquer pessoa, em qualquer lugar no mundo, poderia contribuir para os ataques contra a Geórgia.

E novamente, utilizando-se dos BOTNET`s como estratégia de ataque zumbi cibernético, a Geórgia foi submetida a um bloqueio virtual que derrubou o tráfego de informações digitais do País.

De acordo com Stephen Blank, empreendedor da indústria de tecnologia do Vale do Silício:

> Embora os teóricos russos tenham discutido o que eles chamam de “operação de informação” contra as forças inimigas, o que foi evidenciado na guerra de 2008 com a Geórgia, é que a maioria dos usos reais das “armas de informação em operações” têm visado os "nervos domésticos do governo" ou da sociedade, e não as forças de combate ou o comando e controle militar. Na verdade, o aspecto "informativo-psicológico" que cobre o uso da imprensa e dos meios de comunicação social foi amplamente concebido contra o espaço da informação de um alvo é uma categoria chave entre muitos na definição russa de “operação de informação” e “armas de informação em operações” (BLANK, 2016, p. 219-220).

Em que pese a articulação ofensiva mundial da Rússia, os impactos dos ciberataques à Geórgia foram contidos, uma vez que o governo georgiano conseguiu redirecionar grande parte do seu tráfego de informações para servidores em outros países, como a Estónia, a Polónia e os Estados Unidos da América.

4.1.7. UCRÂNIA (2015): O GRANDE SHUTDOWN.

O conflito político entre Rússia e Ucrânia se intensificou quando o então Presidente ucraniano Viktor Yanukovych recusou-se a assinar, sob influência da Rússia, um acordo de livre-comércio entre Ucrânia e União Europeia, em novembro de 2013. A não assinatura do termo ocasionou a queda e o exílio do Presidente, sob profunda crise política ucraniana.

Aproveitando-se do contexto, a Rússia inicia a intervenção ao território da Crimeia, província ao sul da Ucrânia e de grande valor estratégico, devido ao seu posicionamento com saída para o Mar Negro.

Em 16 de março de 2015, os cidadãos da região da Crimeia decidiram pela anexação do território à Rússia com 96.7% dos votos favoráveis. No entanto, os conflitos na região não cessaram.

Na véspera do natal daquele ano, em 23 de dezembro de 2015, hackers da Sandworms Team – grupo russo de espionagem cibernética que operava desde 2009 - foram os responsáveis por administrar o ataque “BlackEnergy”, através do malware conhecido como KillDisk que literalmente desligou os disjuntores da Ucrânia, deixando mais de 220 mil cidadãos sem energia elétrica, um ato sem precedentes na história.

Os ciberataques foram direcionados a três centros de distribuição da empresa de energia elétrica na Ucrânia Ocidental. Utilizando acesso remoto, os hackers controlaram os computadores dos centros de distribuição e desligaram os disjuntores causando a queda de energia em todo a Ucrânia. Os operadores que estavam na empresa perderam completamente o controle do sistema e não foram capazes de desfazer o dano a tempo. Só lhes coube assistir ao cursor do mouse mexendo “sozinho” e desligando o sistema.

O blackout durou aproximadamente 6 horas, tempo suficiente para se instalar pânico generalizado na população, sem mencionar os danos permanentes a aparelhos eletrônicos por todo o País em decorrência do corte abrupto de energia.

No evento da Crimeia, a Rússia pode ter vislumbrado uma oportunidade, em outras palavras, uma fraqueza na Ucrânia. Trata-se da irrisória participação social nos eventos cibernéticos. Sobre o tema, apresento algumas considerações de Tim

Maurer, co-diretor da Cyber Policy Initiative e membro sênior do Carnegie Endowment for International Peace e Especialista em segurança cibernética e geopolítica da era digital: “o conflito não parece ter mobilizado os atores não-estatais mais sofisticados com recursos cibernéticos na região” (MAURER, 2015, p.84).

Maurer pondera que não se verifica nos cidadãos ucranianos um forte nacionalismo capaz de mobilizar uma reação coordenada entre os *agentes privados “proxy”* (termo por ele criado para designar a gama de atores circulando na esfera cibernética privada) e o governo ucraniano. Em contrapartida, tal situação é facilmente evidenciada na Rússia, que já demonstrou em diversos momentos a habilidade de congregar os agentes do governo e os grupos hackers russos, de forma a atuarem coordenadamente.

Ainda assim, em que pese a capacidade limitada do governo ucraniano, cumulada ao nacionalismo pouco contundente do povo daquela região, é importante observar os contornos externos que este episódio trouxe para os países vizinhos.

A exemplo, cita-se o posicionamento dos países membros da OTAN ao estabelecer o “Cyber Defence Trust Fund” - Fundo Fiduciário de Defesa Cibernética para a Ucrânia, que visa ao apoio necessário para desenvolver estritamente a capacidade defensiva em face de ataques cibernéticos.

Verifica-se, portanto, a preocupação do bloco da OTAN no sentido de auxiliar a ciber defesa na Ucrânia, posicionando-se claramente ao lado de Kiev, e consequentemente, contra Moscou.

4.1.8 CÉLULA TERRORISTA NOS JOGOS OLÍMPICOS DO RIO DE JANEIRO, EM 2016.

Às vésperas das Olimpíadas Mundiais de 2016 a Policia Federal deflagrou a operação HASHTAG na qual monitorava em ação controlada o cotidiano de 50 integrantes de grupo terrorista.

Para captar as informações do grupo, a Polícia Federal infiltrou um agente nos grupos de bate-papo em que os indivíduos articulavam o ataque terrorista durante os Jogos Olímpicos do Rio de Janeiro.

O grupo, autointitulado “Defensores da Sharia”, seguia o mesmo procedimento de atos preparatórios dos crimes terroristas envolvidos nos atentados em Orlando, nos Estados Unidos, e em Paris, na França, e compartilhavam as informações através de aplicativos de troca de mensagens, o que possibilitou à Policia Federal o rastreamento do grupo terrorista.

No dia 21 de julho de 2016, foram cumpridos 12 mandados para prisão temporária, 2 mandados de condução coercitiva e 20 mandados de busca e apreensão em diversos Estados da Federação.

Aplicou-se ao evento de 2016 a análise das informações disseminadas no cyber-espaço e detecção prévia da ação do grupo, modelo defensivo ideal a ser perquirido por uma Nação, eis que aniquila a ameaça ainda em seu estágio embrionário, sem causar alarde, nem frustrar a confiança das instituições e o mais importante, sem danos estruturais e sem vítimas.

4.1.9 O LEVANTAMENTO DAS COMPETÊNCIAS CIBERNÉTICAS BRASILEIRAS

A guerra cibernética é considerada hoje a principal ameaça à segurança nacional. Sendo assim, as iniciativas brasileiras para o aperfeiçoamento das técnicas de defesa cibernética vão ao encontro do protocolo que já vem sendo adotado pelas grandes potências mundiais.

No entanto, considerando a ausência de conflitos territoriais no Estado Brasileiro e a cooperação dos Estados latino-americanos na proteção mutua das soberanias dos países membros do Mercosul, é possível posicionar o ambiente interno de atuação da Guerra Cibernética no contexto das funções de combate com enfoque nas capacidades operativas de proteção e exploração cibernéticas, uma vez que não possuímos, até o presente momento, uma evidencia pública e notória acerca da capacidade operativa de ataque cibernético do Estado Brasileiro.

Importante destacar ainda que os vetores da guerra cibernética que se concentram em proteger e explorar são compostos de ações que ocorrem nos bastidores, de forma silente e sorrateira, eis que eventual divulgação das ações cibernéticas resultaria no próprio fracasso da operação.

Cabe ressaltar a atuação da Polícia Federal na operação HASHTAG, a pouco explicada, que mostra a expertise que este órgão de investigação vem desenvolvendo no monitoramento do espaço cibernético. Numa situação de combate essa competência seria de grande valia para levantar informações negadas a respeito das ações do inimigo. A capacidade de monitorar as comunicações inimigas no meio cibernético, de forma velada, traz a possibilidade de se antecipar às ações do oponente, negando-lhe emprego da surpresa, princípio de guerra de suma importância em combate.

4.1.10 O LEVANTAMENTO DAS COMPETÊNCIAS CIBERNÉTICAS RUSSAS

A Rússia já demonstrou ao mundo inúmeras vezes o seu potencial de cyberwar. Aliados à hackers - que não se intitulam do governo, a Rússia mostrou destreza em articular a guerra cibernética propriamente dita (por meio de ataques com pragas virtuais) com diversas outras ferramentas de informação, sem mencionar as operações militares de guerra convencional como foi o caso da região da Ossetia do Sul, no episódio da Geórgia em 2008.

O levantamento das competências cibernéticas russas, ao que consta experienciado até o momento, vai desde phishing de lança, malware, ataques DDoS, ataques de negação de serviço por telefone (TDoS) e outras formas de interrupção cibernética à espionagem cibernética.

Mas é importante lembrar que o que se sabe sobre potencial cibernético do inimigo é tão somente a ponta do iceberg que, em algum momento, por motivos políticos ou econômicos, precisou ser exposto ao mundo. O maior potencial cibernético, e por consequência o mais danoso, sempre estará sob alto sigilo de interesse nacional e sempre que possível será utilizado sem que ninguém nem ao menos perceba ou se dê conta de que pode estar sendo atacado.

Ainda assim, é importante ressaltar que os ataques cibernéticos às infraestruturas conectadas ao ciberespaço são uma perigosa tendência nas estratégias de guerra contemporâneas e futuras.

4.2 DISCUSSÕES

Da pesquisa bibliográfica realizada, é possível inferir que o estado de guerra cibernética não é algo iminente, mas atual e se revela numa prática constante, sobretudo em suas capacidades operativas de proteção e exploração cibernéticas, que se desenvolvem de forma velada e dão ao inimigo pouca ou nenhuma possibilidade de predição.

Da pesquisa apresentada verificou-se ainda que, no evento havido na Crimeia, um serviço básico e fundamental, como o funcionamento da rede de energia elétrica de em um país europeu, foi corrompido através de uma intrusão eletrônica, dentro do ciberespaço.

O evento mundialmente conhecido como shutdown da Crimeia é uma demonstração prática de como os serviços básicos do Estado estão cada vez mais conectados ao ciberespaço.

A mesma tendência se confirma no Brasil, onde o Estado alcança seus cidadãos por meio dos diversos aplicativos oferecidos pelas plataformas digitais do Governo.

Sendo assim, é importante trazer à discussão o implemento da segurança digital por meio do Sistema de Homologação e Certificação de Produtos de Defesa Cibernética, já que, na medida em que o Governo se digitaliza, torna-se cada vez maior a quantidade de informações, sejam pessoais ou de governo, no ambiente virtual.

Neste sentido, destaca-se o comentário que consta no relatório FOI-R-2970-SE, de março de 2010, apresentado na obra “Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations”, de Roland Heickero:

> As emergentes ameaças cibernéticas mostram o quanto é preciso incrementar tanto a segurança da informação quanto a cooperação internacional no sentido de evitar ou reduzir efeitos negativos de operações cibernéticas antagônicas. O tema ameaça cibernética deve ser resolvido em escala mundial, envolvendo o maior número de partes, de leis, e de agências de todas as Nações. Convenções têm de ser reescritas uma vez que a guerra cibernética confunde princípios como os da proporcionalidade, neutralidade e distinção. As regras cibernéticas necessitam ser melhor discutidas (Heickero, 2010, p. 55).

5. CONSIDERAÇÕES FINAIS

Diante do cenário apresentado, depreende-se que o campo de batalha virtual está em constante expansão, acompanhando o fluxo das descobertas tecnológicas e ganhando destaque face as técnicas tradicionais de batalha cinética.

Um vírus virtual pode comprometer a infraestrutura tecnológica do inimigo, ambiente onde tudo é armazenado, não se compara ao lançamento de um míssil balístico no terreno do inimigo, tal investida traria prejuízo ínfimo quando comparada a uma praga virtual.

Da mesma maneira, um programa malicioso compromete a comunicação de um País de forma sistêmica, com a interrupção do bem mais valioso deste século, a informação. Numa nova comparação, não existe avanço no terreno do inimigo tão veloz que se equipare à velocidade de disseminação de um vírus.

O Campo de estudo das modalidades de guerra cibernética é tão fértil que não se pode afirmar que seria possível dominá-lo, sabotando os sistemas do inimigo e garantindo ao próprio país o uso totalmente seguro desse espaço.

E, sob o mesmo raciocínio, também não seria possível o controle do espaço cibernético por Entidades Públicas Civis, evitando a utilização do meio cibernético para o cometimento de crimes patrimoniais, à imagem ou até mesmo ações terroristas.

No entanto, o que se pode afirmar é que viver em constante estado de guerra cibernética, seja por meio da capacidade operativa de proteção ou exploração, é a medida contemporânea mundialmente adotada para se evitar a guerra cinética.

REFERÊNCIAS

BLANK, Stephen. “Information Warfare a La Russe”, in: *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competitions*, Phil Willians and Dighton Fiddner (Eds.), Strategic Studies Intitute and U.S. Army War College Press, August 2016, 219 – 220.

BRASIL. Decreto Legislativo nº 179 de 14 de dezembro de 2018. Institui a Política Nacional de Defesa. **Diário Oficial da União**: seção 1, Brasília, DF, p. 4-114, 17 dez. 2018.

BRASIL. Decreto nº 10.222, de 05 de fevereiro de 2020. Institui a Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**: seção 1, Brasília, DF, p. 6, 06 fev. 2020.

BRASIL. Decreto nº 9.668, de 02 de janeiro de 2019. Aprova a estrutura regimental do GSIPR. **Diário Oficial da União**: Seção 1, Brasília, DF, Edição Extra – C, p. 1, 02 jan. 2019.

BRASIL. Portaria nº 1.252, de 29 de dezembro de 2017. Aprova o Regimento Interno da Polícia Federal. **Diário Oficial da União**: Seção 1, Brasília, DF, Edição 1, p. 40 – 70, 02 jan. 2018.

BRASIL. Portaria nº 42 – COTER, de 8 de junho de 2017. Aprova o Manual de Campanha de Guerra Cibernética (EB70-MC-10.232)**.** 1ª Edição. 2017. **Boletim do Exército**: 2ª parte, Brasília, DF, n 25, p. 37, 23 jun. 2017.

BRASIL. Portaria nº 45 GSIPR, de 08 de setembro de 2009. Institui o Grupo Técnico de Segurança Cibernética. **Diário Oficial da União**: seção I, Brasília, DF, n. 172 , p. 2, 09 set. 2009.

CIBERGUERRA. In: **WIKIPÉDIA, a enciclopédia livre**. Flórida: Wikimedia Foundation, 2019. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Ciberguerra&oldid=54938432>. Acesso em: 01 abr. 2020.

Cyber Defense Trust Fund. NATO, 2016. Disponível em: < https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160712_1606-trust-fund-ukr-cyberdef.pdf>. Acesso em: 02 de abr. de 2020.

DUNHAM, Ken; MELNICK, Jim. *Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet*. Dallas:CRC Press, 2008.

ESCOSTEGUY, Filipe. Polícia Federal prende célula do Estado Islâmico que planejava atentado na Olimpíada. ÉPOCA, 2016. Disponível em: < https://epoca.globo.com/tempo/noticia/2016/07/pf-prende-celula-do-estado-islamico-que-planejava-atentado-na-rio-2016.html>. Acesso em: 02 de abr. de 2020.

FALCOSKI, Arthur Bolfi. **O ciberespaço, a Rússia e as relações internacionais: o poder cibernético do kremlin e suas consequências globais.** 2017. Trabalho de Conclusão de Curso (Bacharelado em Relações Internacionais)-Universidade Federal do Pampa, Santana do Livramento, 2017.

GERASIMOV, Valery. The Value of Science is in the Foresight. **Military Review**. p. 24, jan./fev., 2016.

GERASIMOV, Valery. The Value of Science is in the Foresight. **Military Review**. p. 27, jan./fev., 2016.

LÉVY, Pierre. *Cibercultura*. 1. ed. São Paulo: Editora 34, 1999. 17 p.

MAURER, T: Cyber Proxies and the Crisis in Ukraine. In: Geers, K (ed.). **Cyber War in Perspective**: Russian Aggression Against Ukraine. p. 79-86 NATO CCDCOE Publications. Tallinn 2015.

MPF acusa oito pessoas de planejar terrorismo para Jogos Olímpicos. CONJUR, 2016. Disponível em: < https://www.conjur.com.br/2016-set-16/mpf-acusa-oito-pessoas-planejar-terrorismo-jogos-olimpicos>. Acesso em: 02 de abr. 2020.

PF INAUGURA CENTRO CONTRA ATAQUES CIBERNÉTICOS. **Site oficial da Polícia Federal**, 2012. Disponível em: < http://www.pf.gov.br/agencia/noticias/2012/junho/pf-inaugura-centro-contra-ataques-ciberneticos>. Acesso em: 02 abr. 2020.

REVISTA EM DISCUSSÃO! Brasília: Senado Federal. Ano 3, n 10, mar. 2012, 38 p.

ROLAND, Heickero. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*. FOI-R, 2970, Stockholm, 2010, p. 55.