ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

ESCOLA DE FORMAÇÃO COMPLEMENTAR DO EXÉRCITO

Cap QCO Infor **Edson** Barbosa de Souza

A GUERRA CIBERNÉTICA E O EXÉRCITO BRASILEIRO: UMA REVISÃO DOUTRINÁRIA

Rio de Janeiro
2019

Cap QCO Infor Edson Barbosa de Souza

A GUERRA CIBERNÉTICA E O EXÉRCITO BRASILEIRO: UMA REVISÃO DOUTRINÁRIA

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau Especialização em Ciências Militares.

Orientador: TC Com RODRIGO LESTINHO ÁVILA

Rio de Janeiro
2019

Cap QCO Infor Edson Barbosa de Souza

A GUERRA CIBERNÉTICA E O EXÉRCITO BRASILEIRO: UMA REVISÃO DOUTRINÁRIA

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau Especialização em Ciências Militares.

Aprovado em

COMISSÃO DE AVALIAÇÃO

_____

RODRIGO LESTINHO ÁVILA– TC Com – Presidente
Escola de Formação Complementar do Exército

_____

ANDERSON BARROS TORRES– Maj - Membro
Escola de Formação Complementar do Exército

A GUERRA CIBERNÉTICA E O EXÉRCITO BRASILEIRO: UMA REVISÃO DOUTRINÁRIA

Cap QCO Infor Edson Barbosa de Souza[a]

RESUMO

A guerra moderna não mais se limita às fronteiras geográficas de um país: a disputa é pelo controle dos sistemas informatizados que hoje são essenciais para a vida das populações, como os sistemas responsáveis pela distribuição de energia elétrica, de água, transporte e pelos serviços de urgência. No contexto da guerra cibernética, cresce a importância de uma nação desenvolver sistemas de defesa visando assegurar a manutenção desses serviços e impedir que as ameaças virtuais se transformem numa realidade caótica. O objetivo deste artigo é discutir os principais conceitos relativos à Guerra Cibernética, analisando os elementos legais internacionais e nacionais envolvendo o tema. A metodologia empregada foi a revisão bibliográfica. Concluiu-se que, um ataque cibernético só deve ser caracterizado como Guerra Cibernética, caso haja um patrocínio de um Estado e que o Exército tem se empenhado em desenvolver regulamentos próprios para o setor Cibernético, além de atuar intensamente na área, destacando-se a participação em grandes eventos como, jogos Olímpicos e Paralímpicos Rio 2016 e a Copa do Mundo de 2014.

Palavras-chave: Guerra Cibernética. Legislação Cibernética. Defesa Cibernética.

ABSTRACT

The modern warfare is no longer confined to a country's geographical borders: the battle is over control of computer systems that are essential to the lives of people today, such as the systems responsible for the distribution of electricity, water, transportation, and services. urgency. In the context of cyber warfare, the importance of a nation developing defense systems to ensure the maintenance of these services and to prevent cyber threats from becoming a chaotic reality grows. The aim of this article is to discuss the main concepts related to the Cyber War, analyzing the international and national legal elements involving the theme. The methodology employed was the literature review. It was concluded that a cyber attack should only be characterized as a cyber war if there is state sponsorship and that the army has been working to develop its own regulations for the cyber sector, as well as intensely acting in the area. participation in major events such as the Rio 2016 Olympic and Paralympic Games and the 2014 World Cup.

Keywords: Cyber War. Cyber Laws. Cyber Defense.

[a] Capitão QCO Informática da turma de 2011. Mestre em Sistemas e Computação pelo Instituto Militar de Engenharia (IME) em 2018.

Sumário

1. INTRODUÇÃO

As ações de *hackers* e os ataques a sites oficiais do Governo Brasileiro são frequentes nos dias atuais:" Anonymous hackeia Ministério da Defesa e expõe dados de Villas Boas e Mourão" (WAKKA, 2018). Em Setembro de 2019, celulares do presidente Bolsonaro foram alvos de grupos de hackers (BORGES, 2019).

Pela ótica de mídia, a segurança da informação e a estabilidade dos sistemas informatizados nunca foram tão questionadas no Brasil. Nos meios de comunicação em geral, guerra cibernética (ou ciberguerra) e ataque *hacker* são sinônimos e a preparação dos órgãos de defesa diante dessas ameaças é constantemente questionado. Para além da opinião pública, é responsabilidade do Exército Brasileiro, pela Estratégia Nacional de Defesa (MINISTÉRIO DA DEFESA, 2012), atuar no campo da segurança da informação e assegurar que o País estará preparado para a guerra do século XXI, na qual as redes de computadores são meio e teatro de operações.

A defesa da soberania nacional é dever constitucional das Forças Armadas. A atual conjuntura internacional, com os avanços na área de Tecnologia da Informação e Eletrônica, traz novas possibilidades e maiores desafios para o Exército, Marinha e Aeronáutica (LIMA, 2018). Em uma provável guerra cibernética que envolvesse o Brasil, alvos cruciais seriam as "infraestruturas críticas", ou seja, os setores energético, financeiro, bancário, de transportes, telecomunicações, fornecimento de água, rede hospitalar, órgãos de defesa, segurança pública e polos tecnológicos (DA SILVA, 2019). Mesmo para os dirigentes desses setores, seria difícil garantir que já há o preparo necessário para evitar que as ameaças virtuais tenham efeitos reais num conflito. Portanto, eles se constituem em vulnerabilidades. Assim sendo, em Fevereiro de 2019, o Exército Brasileiro ativou a Escola Nacional de Defesa Cibernética, a fim de aumentar a oferta de treinamentos na área (LOPES, 2019).

O objetivo do presente artigo é discutir os conceitos e a legislação nacional e internacional relacionados à Guerra Cibernética, por meio de revisão bibliográfica do tema.

1.1. PROBLEMA

Para considerar-se Guerra Cibernética basta que algum sistema crítico de um país seja invadido por *hackers*? Sabe-se que a guerra tradicional é regulamentada por diversas leis do Direito Internacional Humanitário (DIH) ou Direito Internacional

dos Conflitos Armados (DICA), compostos pelas Convenções de Genebra e da Convenção de Haia. Qual o análogo para a Guerra Cibernética? Quais os seus limites?

1.2. OBJETIVO GERAL

O presente estudo pretende integrar os conceitos básicos e a informação científica relevante e atualizada, a fim de fazer uma revisão nos conceitos de Guerra Cibernética e na responsabilidade do Exército Brasileiro no cenário da guerra da informação, segundo a Estratégia Nacional de Defesa.

1.2.1. Objetivos Específicos

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

a. Definir a origem do termo Guerra Cibernética.
b. Analisar os contextos de emprego de Guerra Cibernética.
c. Discutir o conceito de Guerra Cibernética.
d. Analisar a legislação referente a Guerra Cibernética.
e. Avaliar o papel do Exército Brasileiro no cenário da Guerra Cibernética à luz da legislação de referência.

1.3. QUESTÕES DE ESTUDO

a. O que é Guerra Cibernética?
b. Qual a diferença entre Guerra Cibernética e as Guerras tradicionais?
c. Quais são os limites legais para a Guerra Cibernética?
d. Qualquer tipo de ataque *hacker* pode ser considerado Guerra Cibernética?
e. Guerra Cibernética é algo isolado ou é parte de uma operação militar mais ampla?
g. Como as legislações mundiais tratam da Guerra Cibernética?

As respostas aos questionamentos anteriormente apresentados guiarão o presente trabalho, a fim de elucidar de uma maneira mais didática o presente problema apresentado.

1.4. JUSTIFICATIVA

A presente pesquisa justifica-se pela necessidade de desenvolver um trabalho

investigativo acerca da abrangência do tema, a fim de compreender o Conceito de Guerra Cibernética, dentro do contexto militar, relacionando-o às responsabilidades da Força alicerçadas pelo Plano de Estratégia Nacional de Defesa.

O que impulsionou a realização deste trabalho foi o entendimento de que a Guerra Cibernética é um assunto atual, que em função de dispositivos legais tornou-se atribuição do Exército Brasileiro e, portanto, direta ou indiretamente deve ser de conhecimento de todos os integrantes da Força Terrestre. Assim como a Segurança da Informação não é responsabilidade exclusiva do pessoal de Tecnologia da Informação de uma corporação, entender o conceito de Guerra Cibernética e como ela se insere no contexto de uma operação militar, ajudará a conscientizar os soldados de Caxias de seu papel no cenário da guerra do século 21.

2. REFERENCIAL TEÓRICO

THORNTON (2019) afirma que há diversas redes que estariam na linha de frente de uma possível guerra cibernética: redes de distribuição de energia elétrica; redes de distribuição de água potável; redes de direção das estradas de ferro e metrôs; redes de direção do tráfego aéreo; redes de tráfego urbano; redes de informação de emergência, como prontos-socorros, polícias, bombeiros e defesa civil; redes bancárias, podendo, por exemplo, apagar o dinheiro registrado em nome dos cidadãos; redes de comunicações, como estações de rádios, televisão; *links* com sistemas de satélites artificiais, como os fornecedores de sistemas telefônicos, de sinais para televisão, de previsões de tempo e de posicionamento global (GPS); redes do Ministério da Defesa ou outros considerados chave, como Justiça, Integração Nacional e Meio Ambiente; redes do Banco Central, sistemas de ordenamento e recuperação de dados nos sistemas judiciais, incluindo os de justiça eleitoral.

Nunes (1999) situa a guerra cibernética como parte da guerra eletrônica, sendo definida como “a utilização de todas as ferramentas disponíveis ao nível da eletrônica e da informática para derrubar os sistemas eletrônicos e de comunicações inimigos e manter os nossos próprios sistemas operacionais” (NUNES, 1999). Para Parks e Duggan (2000), a guerra cibernética é o subconjunto da guerra da informação que envolve ações realizadas no mundo cibernético (Internet e as redes a ela relacionadas, as quais compartilham mídia com a Internet).

Na próxima seção, será discutida a relação entre a Guerra Cibernética e a Segurança da Informação.

2.1. A SEGURANÇA DA INFORMAÇÃO

Muitos sistemas de armas e de comunicações militares dependem da velocidade e funcionalidade oferecidas pelas redes de computadores para garantir sua operacionalidade. No campo da tomada de decisões militares, informações são trocadas por dispositivos passíveis de acesso remoto, o que pode ser explorado por um atacante. Além disso, e principalmente, estão no alvo os sistemas civis que, se atingidos, poderiam paralisar redes de distribuição de energia elétrica, por exemplo, ou o acesso aos bancos. Em qualquer das hipóteses, os ataques causariam uma desordem generalizada e pânico na população, cenário propício para outras formas mais tradicionais de efetivação do conflito, como avanço por terra ou bombardeios (WEINER, 2018). Apesar de serem alvos majoritariamente civis, os sistemas críticos, uma vez penetrados, poderiam inviabilizar toda uma estratégia de defesa e levar um país à rendição por “total paralisia estratégica” (OLIVEIRA JUNIOR, 2011). Na área militar, alvos preferenciais seriam sistemas de comando e o controle dos sistemas de armas das forças em operação, comprometendo, assim, a capacidade de coordenação das ações e o poder de fogo.

O contexto da eliminação de fronteiras proporcionado pela Internet ainda é fonte de desafios para as instituições de combate ao crime, uma vez que facilitou a ocorrência de crimes eletrônicos onde a vítima e o criminoso encontram-se em países distintos (VIEIRA, 2018). As ameaças e as vulnerabilidades no campo da guerra cibernética também podem ser inseridas numa área do conhecimento mais ampla, a Segurança da Informação (WIENER, 2018). Afinal, mesmo que não estejam inseridas num contexto de guerra, os sistemas e as redes de computadores podem estar abertos a ameaças internas. A Segurança da informação tem como objetivos manter a integridade (esta não foi modificada ao longo do caminho), disponibilidade (a informação está sempre acessível pelos usuários autorizados) , confidencialidade (a informação estará acessível apenas para pessoas autorizadas) e não-repúdio da informação (uma vez enviada uma mensagem, seu emissor não pode negar a autoria da mesma) (STALLING, 2015).

Segundo STALLING (2015) ameaça no campo da Segurança da Informação é definida como a possibilidade de exploração de fragilidades de sistemas, de forma

intencional ou não, de origem interna ou externa; quando ocorre a efetivação da ameaça, tem-se um ataque. As ameaças podem ser classificadas em várias categorias, como violação de autorização (utilização de uma autorização para outra finalidade); recusa de serviços (não atendimento, sem motivo explícito, das requisições de usuários legítimos); espionagem (obtenção de informação, sem autorização do proprietário); vazamento (revelação indevida de informação); violação de integridade (modificação não autorizada de informação); mascaramento (passar-se por outro); *replay* (retransmissão ilegítima); repudiação (negação imprópria de uma ação ou transação efetivamente realizada); exaustão (sobrecarga de utilização de recurso); emulação (imitação para conseguir informações sensíveis); roubo (posse ilegítima de informações); *backdoor* (programação inserida e escondida no sistema, que possibilita um acesso de forma não convencional) e cavalo de tróia (programa de captura indevida de informações) (STALLING, 2015).

Esses tipos de ameaças possibilitam ataques, que podem ser caracterizados como: invasão (acesso intencional e não justificado, por pessoa não autorizada pelo proprietário ou operadores dos sistemas); interceptação (acesso não autorizado à transmissões, possibilitando a cópia das mensagens transmitidas, sendo o ataque mais comum e de difícil detecção pelas partes legítimas); modificação (é um agravante da interceptação, em que o conteúdo da mensagem é alterado); fabricação (simulação para o destino de uma origem legítima, em que o atacante faz-se passar por uma procedência legítima, inserindo objetos espúrios no sistema atacado) e indisponibilidade ou interrupção (ações não autorizadas ocasionado sobrecarga no processamento de sistemas, tornando-os inacessíveis aos legítimos usuários, por longos períodos ou por sucessões de pequenos intervalos) (STALLING, 2015).

2.2. A GUERRA CIBERNÉTICA

STOPATTO (2009) afirma que uma guerra por vias cibernética, é caracterizada pela disputa entre nações, ou seja, existe o papel de um Estado.

De acordo com WHYTE (2018), ciberguerra é "o uso de qualquer arma (cibernética) por um Estado contra o território de outro Estado". STONE (2013), comenta que a distinção sobre se um ataque cibernético é um ato de guerra, criminalidade ou espionagem, está intimamente relacionado ao entendimento do conceito de guerra, que deve ter motivação política e ter um potencial de letalidade, afinal, a guerra pode

ser entendida como um ato de força para obrigar o inimigo submeter-se a nossa vontade. GOMPERT (2019) enfatiza que embora uma grande variedade de atores não estatais se envolva em guerra cibernética, esta só é caracteriza com participação de um Estado e nos alerta que as principais potências cibernéticas são, por coincidência, as maiores potências em armas nucleares. Para FINLAY(2018), ciberguerra é definida pelos ataques no espaço cibernético que produzam algum efeito cinético, não mencionando a autorização estatal.

O manual de Guerra Cibernética do Exército Brasileiro define:

> GUERRA CIBERNÉTICA corresponde ao 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 para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios (BRASIL, 2017, p.18).

Apesar de diversidade de definições é notória a existência de um aspecto consensual, onde para ocorrer uma Guerra Cibernética, é necessário um patrocínio estatal, pois as ações oriundas de um indivíduo com motivações pessoais, não podem ser consideradas como Guerra Cibernética, embora possam ser igualmente prejudiciais (JOHNSON, 2015; KIM, 2019; McCARTHY, 1981; ROBINSON, 2015; STOPATTO, 2009; WANG, 2019).

De acordo com BRASIL (2017), a guerra cibernética conduzida por componentes especializados das forças armadas nos níveis operacional e tático, busca contribuir para as ações mais amplas da defesa cibernética. O Comando de Defesa Cibernética (ComDCiber), órgão central do Sistema Militar de Defesa Cibernética, coordena e integra esses componentes das forças singulares, buscando viabilizar o exercício do Comando e Controle (C2), por meio da proteção dos ativos de informação, além de negar o exercício do C2 do oponente.

No contexto do Ministério da Defesa, as ações no espaço cibernético deverão ter as seguintes denominações, de acordo com o nível de decisão (BRASIL, 2017):

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.

Em pesquisa desenvolvida a pedido da Força Aérea dos Estados Unidos, LIBICKI (2009, p. 13) classifica as ameaças que constituem ciberataques em "externas" e "internas". As externas vêm de fora do sistema e são mais bem representadas pela ação dos *hackers,* enquanto as internas são representadas pelos *backdoors*[1]*.* Pela análise do autor, este seria o caminho mais esperado a ser tomado por um Estado, especialmente quando o alvo no território inimigo fosse civil. Dessa forma, é possível furtar dados, ou mesmo instalar um código que permita um futuro controle da máquina. Uma outra possibilidade é "enganar" a máquina implantando um código que a faça funcionar inadequadamente, chegando a corromper e até destruir seu funcionamento. Pode-se relembrar o episódio em que o FBI alertou o governo e empresas americanas que a suíte de segurança russa Kaspersky poderia espionar computadores (CUNHA LEITE, 2014).

De acordo com o Glossário das Forças Armadas (BRASIL, 2010), defesa é entendida como "o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança", ou ainda, como "reação contra qualquer ataque ou agressão real ou iminente". O mesmo glossário define ataque como "ato ou efeito de dirigir uma ação ofensiva contra o inimigo" e Guerra Cibernética como

> Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores (BRASIL, 2011,p.134)

Assim como na Guerra Tradicional, o combate cibernético segue alguns princípios que serão descritos agora, na mesma qualificação adotada por Cahill, Rozinov e Mule (2003), PINHEIRO (2010) e (OLIVEIRA, 2010):

[1]programação inserida e escondida no sistema, que possibilita um acesso de forma não convencional

Princípio da Mutabilidade: Não existem leis de comportamento imutáveis no mundo cibernético, excetuando-se aquelas que necessitam de uma ação no mundo real.;

Princípio do Disfarce: Alguma entidade no mundo cibernético possui a autoridade, acesso, ou habilidade que um atacante deseja realizar; o objetivo deste é assumir a identidade dessa entidade;

Princípio da Dualidade do Armamento: As ferramentas de Guerra Cibernética são duais, ou seja, usadas por atacantes e administradores de sistemas com finalidades distintas;

Princípio da Compartimentação: O atacante e o defensor de um sistema controlam uma pequena fração do ciberespaço que utilizam;

Princípio da Usurpação: Controlar a parte do ciberespaço que o oponente utiliza, significa controlar o oponente;

Princípio do Efeito Cinético: uma ação da guerra cibernética precisa ter efeito vantajoso para o atacante no mundo real;

Princípio da Proximidade: para realizar uma ação no mundo cibernético não é necessária uma proximidade física, diferentemente de que ocorre com uma ação cinética;e

Princípio da Incerteza: nunca é possível saber, com total certeza, se o próximo passo numa ação cibernética logrará êxito, já que nem sempre os programas e os equipamentos trabalharão da forma esperada.

2.3. A GUERRA CIBERNÉTICA E O DIREITO INTERNACIONAL

A fim de compreender o contexto atual da Guerra Cibernética, é necessário estudá-la também do ponto de vista das legislações nacional e internacional.

Em seu artigo 142, a Constituição brasileira define que:

> As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas, com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República, e destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem (BRASIL, 1988).

A defesa da soberania do país é dever das Forças Armadas, de acordo com o ordenamento jurídico nacional. Do ponto de vista do Direito Internacional ainda não há leis ou acordos específicos sobre a ciberguerra. O fato de uma atividade militar não ser especificamente regulada não quer dizer que esta possa ser usada em confrontos sem qualquer limitação, o que decorre do princípio da humanidade, segundo o qual não se pode aplicar nenhuma punição que inflija a dignidade da pessoa humana (COELHO, 2013). Embora não haja uma regulamentação oficial sobre o tema, existe um documento acadêmico denominado Manual Tallinn, publicado em 2013, que versa sobre aplicação de leis internacionais na Guerra Cibernética (EFRONY, 2018). Em seu artigo 139, por exemplo, o manual de Tallinn diz que “Jornalistas civis envolvidos em missões profissionais perigosas em áreas de conflito armado são civis e devem ser respeitados como tal, em particular no que diz respeito a ciberataques, desde que não participem diretamente nas hostilidades” (SCHMITT, 2013).

Segundo BHATELE (2019), ataques cibernéticos estão sujeitos aos regulamentos do Direito Internacional dos Conflitos Armados (DICA) da mesma forma que estarão sujeitos quaisquer novos tipos de armamento ou método que venham a ser usado nos conflitos bélicos. Em suma, para o DICA a relevância de um ataque é medida mais pelos seus efeitos que pelo modo como ele é perpetrado.

Para que as Convenções e princípios sejam aplicados, deve ser utilizada a analogia de forma a serem definidos o que são alvos militares no campo de batalha cibernético e sejam excluídos destes ataques sistemas de estabelecimentos que comprometam diretamente a população civil, como os de saúde, cumprindo o que dispõe o art. 57, I do Protocolo Adicional I ao prescrever que: “as operações militares devem ser conduzidas procurando constantemente poupar a população civil, as pessoas civis e os bens de caráter civil” (SEITENFUS, 2009) . O artigo 36 do Protocolo I, de 1977, adicional às Convenções de Genebra diz que:

> Quando uma Alta Parte Contratante estude, desenvolva, adquira ou adote uma nova arma, ou novos meios ou métodos de combate, terá a obrigação de verificar se seu emprego, em certas condições ou em todas as circunstâncias, estaria proibido pelo presente Protocolo ou por qualquer outra norma de Direito Internacional aplicável a essa Alta Parte Contratante. (BRASIL, 1993, Art.36)

Deve-se salientar que, assuntos de segurança cibernética também são observados dentro das relações internacionais. O exemplo mais atual foi a proposta da Alemanha e Brasil sobre privacidade da internet na Organização das Nações Unidas (ONU). Essa proposta foi feita à ONU em 2013, pouco tempo após as revelações de Snowden sobre as atividades de espionagem da NSA(*National Security Agency*: Agência de Segurança Nacional), e virou resolução em 2014, durante a 69ª Assembleia Geral (O Globo, 2014).

3. METODOLOGIA

Foi utilizado o método de revisão sistemática da Literatura na área de Guerra Cibernética com a finalidade de analisar os principais conceitos e discutindo os elementos legais internacionais e nacionais envolvendo o tema, através de um estudo profundo de artigos contidos no Portal Capes, utilizando os autores mais precípuos da área. A pesquisa bibliográfica teve como propósito explorar as principais teorias do tema Guerra Cibernética, investigando o estado da arte no campo de ciberguerra.

O critério de seleção dos artigos foi o número de citações dos mesmos nas bases de pesquisa.

4. A ATUAÇÃO DO EXÉRCITO BRASILEIRO NA GUERRA CIBERNÉTICA

A Estratégia Nacional de Defesa (MINISTÉRIO DA DEFESA, 2012) aborda a imprescindibilidade dos três setores decisivos para a defesa nacional na atualidade: o cibernético, o espacial e o nuclear. No que concerne ao papel do primeiro setor, objeto do presente estudo, tem-se que sua meta, numa atividade conjunta com o setor espacial, é atingir a autonomia necessária para visualizar o próprio Estado Brasileiro, sem depender de tecnologia estrangeira, assim como, permitir que as três Forças possam, em conjunto, atuar em rede, guiadas por monitoramento feito a partir do espaço.

Nos termos da Estratégia Nacional de Defesa (MINISTÉRIO DA DEFESA, 2012), coube ao Exército Brasileiro (EB) a responsabilidade pelo trato da área Cibernética.

Assim sendo, o projeto priorizará a força de comunicação entre os efetivos das Forças Armadas e os veículos espaciais, devendo, também, gerenciar o desdobramento da capacitação cibernética nos campos industrial e militar. Saliente-se que a incumbência das Forças Armadas, especificamente do EB, nessa questão Nacional, tem como base normativa autorizadora principal, o artigo 142, da atual Constituição Federal.

CARDOSO (2019) destaca a criação do Centro de Defesa Cibernética (CDCiber), em 2012, através da Portaria Normativa nº 666 de 4 de agosto de 2010, e o trabalho proativo no monitoramento do espaço cibernético brasileiro, além da atuação em grandes eventos ocorridos no Brasil, como a Rio+20, a Copa do Mundo de 2014, os jogos Olímpicos e Paralímpicos Rio 2016.

O Comando do Exército, de forma a atuar mais ostensivamente no campo da ciberguerra, criou em 2012, o Centro de Defesa Cibernética(CDCiber), que é vinculado ao Ministério da Defesa. Desde a sua criação, o CDCiber tem firmado acordos e parcerias com órgãos governamentais e empresas privadas, para a troca de conhecimentos. Em 2014, por exemplo, o CDCiber e o SERPRO(Serviço Federal de Processamento de Dados) assinaram um acordo de cooperação de modo a facilitar o intercâmbio de informações em Defesa Cibernética e processamento de dados (DEFESA, 2014). CARDOSO (2019) destaca que nos últimos grandes eventos realizados no Brasil, a Copa do Mundo de 2014, os jogos Olímpicos e Paralímpicos Rio 2016 e Rio+20, o CDCiber trabalhou em cooperação com a Polícia Federal e a ABIN(Agência Brasileira de Inteligência) recebendo e colaborando com informações de inteligência, que permitiram a realização dos eventos com sucesso.

5. RESULTADOS E DISCUSSÃO

As ameaças e as vulnerabilidades no campo da ciberguerra podem, similarmente, ser incorporadas em uma área do conhecimento mais abrangente, a Segurança da Informação, uma vez que, mesmo que não estejam inseridas em um contexto bélico, os sistemas e as redes de computadores podem estar vulneráveis a ameaças internas.

Embora não haja um consenso sobre a definição de Guerra Cibernética, pode-se observar que há em comum entre os diversos autores que é necessária a existência de patrocínio estatal para que ocorra a Guerra Cibernética. Há uma clara separação entre os mundos cibernético (ou virtual) e cinético (ou real), não obstante,

a ação em um mundo afete o outro e vice-versa. O tema Guerra Cibernética é, portanto, bastante extenso, englobando circunstâncias antes limitadas apenas ao mundo real, incluindo a ameaça à soberania de um país, por exemplo. A Estratégia Nacional de Defesa delegou ao Exército Brasileiro a responsabilidade pelo setor Cibernético no país.

Destaca-se também que, embora não haja ainda uma regulamentação oficial sobre a Guerra Cibernética, existe um tratado acadêmico conhecido como Manual Tallinn, que discorre sobre a aplicação de leis e tratados internacionais à ciberguerra.

6.LIMITAÇÕES DA PESQUISA

Tendo em vista o formato do presente estudo – TC (Trabalho de Conclusão) - realizar um estudo comparativo das doutrinas cibernéticas de outros países, para constatação de exceções ou diferenças está para além do escopo do presente trabalho. Entende-se que a reprodução desses estudos contribuiria para elucidar não só especificidades em contexto brasileiro, mas também ofereceria a oportunidade de desenvolver sugestões para a evolução da doutrina cibernética do Exército Brasileiro, no entanto, a presente pesquisa limitou-se a discutir o conceito de Guerra Cibernética, analisando e discutindo as definições de diferentes autores.

7. CONCLUSÃO

Ao analisar o tema, discorreu-se sobre a Defesa Cibernética que tem a atribuição de obstar as tentativas de ataques virtuais a sistemas críticos, sejam civis ou militares no país.

Demonstrada a relevância do tema em um contexto nacional, evidenciou-se o conceito de Guerra Cibernética, que pode ser sumarizado como o uso do espaço cibernético em operações militares, notoriamente com um patrocínio estatal.

Realçou-se, também, a atuação do Exército Brasileiro para cumprir as suas responsabilidades no setor Cibernético, tanto na parte de aperfeiçoamento dos seus recursos humanos, com cursos voltados a Guerra Cibernética, quanto agindo proativamente, monitorando constantemente o Espaço Cibernético do país.

Os ataques no campo cibernético estão sujeitos aos regulamentos do Direito Internacional Humanitário da mesma maneira que estarão sujeitos quaisquer novos tipos de armamento ou métodos que venham a ser usado nos conflitos.

Como proposta de trabalho futuro, sugere-se o estudo da estrutura e Doutrina cibernética de outros países, como Rússia, China e Estados Unidos e a sua comparação com a realidade brasileira.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil, de 5 de outubro de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 28 jun. 2019.

BRASIL. **Decreto 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências.

BRASIL. **Decreto nº 5.484, de 30 de junho de 2005**. Aprova a Política Nacional de Defesa. Disponível em: < https://www.defesa.gov.br/estado-e-defesa/politica-nacional-de-defesa >. Acesso em: 10 mai 2019.

BRASIL. Ministério da Defesa. EB70-MC-10.232. **Manual de Campanha de Guerra Cibernética**. Brasília,2017.

BRASIL. **Portaria nº 45 PR/GSI, de 8 de setembro de 2009**. Instituiu o Grupo Técnico de Segurança Cibernética, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN).

BRASIL, **Portaria Normativa nº 333/MD, de 24 de março de 2004**. Dispõe sobre a Política de Guerra Eletrônica de Defesa.

BRASIL. Ministério da Defesa. **Glossário das Forças Armadas**. MD35-G-01, v. 4, 2010.

BACH DA GRAÇA, Ronaldo. **Regulação da Guerra Cibernética e o Estado Democrático de Direito no Brasil**. Revista de Direito, Estado e Telecomunicações, v. 6, n. 1, 2014.

BHATELE, Kirti Raj Raj et al. **The Fundamentals of Digital Forensics and Cyber Law**. In: Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems. IGI Global, 2019. p. 21-44.

BORGES, Stella. **Ministério da Justiça diz que celulares de Bolsonaro foram alvo de hackers**. 2019. Disponível em: <https://noticias.uol.com.br/politica/ultimas-noticias/2019/07/25/ministerio-da-justica-diz-que-celulares-de-bolsonaro-foram-alvo-de-ataque.htm>. Acesso em: 13 out. 2019.

CAHILL, Thomas P.; ROZINOV, Konstantin; MULE, Christopher. **Cyber warfare peacekeeping**. In: IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003. IEEE, 2003. p. 100-106.

CARDOSO, Luiz Henrique Filadelfo; ZIGUNOW, Lucas Maurício Alves. **Implementação de testes de invasão em apoio à proteção cibernética de redes e sistemas de interesse da Defesa**. O Comunicante, v. 9, n. 1, p. 23-32, 2019.

CLARKE, Richard A; KNAKE. Robert K. **Cyber War: the next threat to national security and what to do about it**. 2010. Harper Collins E-Books.

COELHO, Teresa Leal. **O Direito Internacional e a Ingerência Humanitária: o poder/dever da intervenção armada**. Nação e Defesa, 2013.

CUNHA LEITE, Alexandre César; OLIVEIRA, Solsona; RAIARA, Ahmina. **Conflitos Cibernéticos: um overview sobre a participação asiática recente**. Meridiano 47-Boletim de Análise de Conjuntura em Relações Internacionais, v. 15, n. 144, 2014.

DA CRUZ JÚNIOR, Samuel César. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Texto para Discussão, Instituto de Pesquisa Econômica Aplicada (IPEA), 2013.

DA SILVA PF. **A Guerra do Futuro já começou e o Brasil enfrenta o desafio do abismo tecnológico**. Centro de Estudos Estratégicos do Exército: Análise Estratégica. 2019 Feb 25;11(1):25-32.

DEFESA, Ministério da. **CDCiber e Serpro assinam acordo de cooperação**. 2014.

Disponível em: <https://www.defesa.gov.br/noticias/8799-cdciber-e-serpro-assinam-acordo-de-cooperacao>. Acesso em: 23 out. 2019.

FINLAY, Christopher J. **Just war, cyber war, and the concept of violence**. Philosophy & Technology, v. 31, n. 3, p. 357-377, 2018.

GLOBO, O. **Onu aprova resolução proposta por Brasil e Alemanha sobre privacidade on-line.** 2014. Disponível em: <https://oglobo.globo.com/economia/onu-aprova-resolucao-proposta-por-brasil-alemanha-sobre-privacidade-on-line-14678862>. Acesso em: 19 out. 2019.

GOMPERT, David C.; LIBICKI, Martin. **Cyber War and Nuclear Peace**. Survival, v. 61, n. 4, p. 45-62, 2019.

JOHNSON, Thomas A. **Cyber Intelligence, Cyber Conflicts, and Cyber Warfare. Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare**, v. 155, 2015.

KIM, Sin-Kon; CHEON, Sang-Pil; EOM, Jung-Ho. **A leading cyber warfare strategy according to the evolution of cyber technology after the fourth industrial revolution**. International Journal of Advanced Computer Research, v. 9, n. 40, p. 72-80, 2019.

LEMOS, A. B. **Forças armadas fortalecem a ciberdefesa do país**. 2016. Disponível em: <https://dialogo-americas.com/pt/articles/brasil-forcas-armadas-fortalecem-ciberdefesa-do-pais>. Acesso em: 18 out. 2019.

LIMA, VICTOR HUGO. **"Hacktivismo e a Defesa Cibernética do Brasil**." *Centro de Estudos Estratégicos do Exército: Análise Estratégica* 8.2 (2018): 12-18.

LIBICKI, Martin C**. Cyberdeterrence and cyberwar**. Rand Corporation, 2012.

LOPES, ADRIANO**. Exército Brasileiro realiza ativação da Escola Nacional de Defesa Cibernética**. 2019. Disponível em: <https://mundohacker.net.br/exercito-

brasileiro-realiza-ativacao-da-escola-nacional-de-defesa-cibernetica/>. Acesso em: 18 out. 2019.

MINISTÉRIO DA DEFESA**. Estratégia Nacional de Defesa**. Disponível em < https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>, Acessado em: 20.10.2019.

OLIVEIRA JUNIOR, Alfredo Ferrão de. **A "guerra cibernética" e o seu emprego pelo Exército Brasileiro na defesa nacional**. Revista do Exército Brasileiro, Rio de Janeiro, Vol. 147, p. 66-79, 1º quadrimestre de 2011.

PINHEIRO, Gen Bda Alvaro de Souza. **A tecnologia da Informação e a Ameaça Cibernética**. In: Revista das Ciências Militares: Fluxo Logístico e Militar Terrestre - Ensinamentos da Logística Empresarial. (2008).

ROBINSON, Michael; JONES, Kevin; JANICKE, Helge. **Cyber warfare: Issues and challenges**. Computers & security, v. 49, p. 70-94, 2015.

SANTOS, Daniel Mendes Aguiar et al. **A arte da guerra no século XXI**. Coleção Meira Mattos: revista das ciências militares, v. 13, n. 46, p. 83-105, 2019.

SARI, Arif; ATASOY, Ugur Can. **Taxonomy of Cyber Attack Weapons, Defense Strategies, and Cyber War Incidents**. In: Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism. IGI Global, 2019. p. 1-45.

SCHMITT, Michael N. (Ed.). **Tallinn manual on the international law applicable to cyber warfare**. Cambridge University Press, 2013.

SEITENFUS, RICARDO. **Legislação internacional**. Editora Manole Ltda, 2009.

STONE, John. Cyber war will take place!. Journal of Strategic Studies, v. 36, n. 1, p. 101-108, 2013.

STALLING, WILLIAM. **Network Security Essentials: Applications and Standards**

Prentice Hall. New Jersey, 2015.

THORNTON, Rod; MIRON, Marina. **Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom**. Journal of Cyber Policy, v. 4, n. 2, p. 257-274, 2019.

WAKKA, Wagner. **Anonymous hackeia Ministério da Defesa e expõe dados de Villas Boas e Mourão.** 2018. Disponível em: <https://canaltech.com.br/hacker/anonymous-hackeia-ministerio-da-defesa-e-expoe-dados-de-villas-boas-e-mourao-123398/>. Acesso em: 12 out. 2019.

WALKER, George K. **Information warfare and neutrality**. Vanderbilt Journal of Transnational Law (ISSN: 0090-2594), Nashville, vol. 33, n. 5, p. 1200. Maio de 2000.

WANG, Weiwei; WU, Lan. **Remove the Confusion and Speed up the Construction of Battlefield Cyber Warfare Force**. In: Recent Developments in Intelligent Computing, Communication and Devices. Springer, Singapore, 2019. p. 1011-1015.

WHYTE, Christopher; MAZANEC, Brian. **Understanding Cyber Warfare: Politics, Policy and Strategy**. Routledge, 2018.

WIENER, Norbert. **Cibernetics: or Control and Communication in the Animal and the Machine**. MIT Press, 1965.

WIENER, Norbert. ***La cibernetica***. Armando Editore, 2018.

WHYTE, Christopher; MAZANEC, Brian. **Understanding Cyber Warfare: Politics, Policy and Strategy**. Routledge, 2018.