9. O emprego da guerra cibernética nas operações militares

2º Sgt. Com. 501 Isaque da Costa Almeida
2º Sgt. Com. 502 Rafael Acioli de Andrade
2º Sgt. Com. 503 Vadson Sampaio da Silva
2º Sgt. Com. 504 Josias dos Santos Azarias Júnior
2º Sgt. Com. 505 Clécio Bernardo Bragança

1. INTRODUÇÃO

A Guerra Cibernética (G Ciber) corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle (C2) do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. 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 à TIC. (DEFESA CIBERNÉTICA, 2014).

Desde a década de 70, a Revolução Informacional elevou o campo virtual a uma nova condição, principalmente relacionado aos assuntos de defesa e segurança. Nações se aparelharam e desenvolveram doutrinas militares aplicadas ao espaço cibernético. Assim, coube ao Exército Brasileiro (EB), da mesma forma, acompanhar essa evolução e traçar objetivos para desenvolver o seu setor cibernético.

O espaço cibernético é, hoje, uma valiosa fonte de informação em qualquer nível. Os ataques aos sistemas de tecnologia da informação e comunicações de um Estado soberano podem causar danos de grande vulto, como o ocorrido em outubro de 2017 aos Estados Unidos da América (EUA), por parte de hackers norte-coreanos (GAZETA DO POVO, 2017).

As ações no espaço cibernético possuem diferentes níveis de atuação, que vão do político ao tático, sendo este último o escalão no qual se enquadra a G Ciber, gerando, assim, impacto nas operações das Forças Terrestres Componentes (FTC).

A FTC, por sua vez, é o elo entre o nível operacional e tático, constituindo um comando operativo coordenador das operações terrestres e elemento essencial no combate moderno. Ainda, o combate terrestre, como missão precípua do EB e, por consequência, da FTC, pode ser conduzido por meio de ações ofensivas ou defensivas. De acordo com o manual de Doutrina Militar Terrestre (BRASIL, 2014), as operações defensivas devem ser executadas até o momento em que se possa retomar a ofensiva, deixando claro que esta é a prioridade no emprego convencional da Força. A FTC é o braço terrestre de um Comando Operacional, sendo responsável por assimilar os objetivos operacionais e, em última análise, cumprir a missão atribuída pelo escalão superior. E para desempenhar com sucesso essa atribuição, a FTC faz uso do poder de combate.

Este trabalho se propôs a apresentar, mediante pesquisa em diferentes fontes de consultas, tais como manuais militares, páginas eletrônicas e dissertações, as principais ações desenvolvidas pelo Exército Brasileiro no desenvolvimento da doutrina de Guerra Cibernética e seu emprego nas operações básicas, apresentando de forma sucinta como a exploração do espaço cibernético se tornou um vertente de vital importância para o aumento do poder de combate da Força Terrestre.

2 FUNDAMENTOS DA GUERRA CIBERNÉTICA

A seguir estão os termos mais aplicados no contexto da G Ciber:

a) AMEAÇA CIBERNÉTICA – causa potencial de um incidente indesejado, que pode resultar em dano ao espaço cibernético.
b) DEFESA CIBERNÉTICA – conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo MD, com as finalidades de proteger os sistemas de informação (Sist Info) de interesse da Defesa Nacional, obter dados para a produção de conhecimento de inteligência e comprometer os sistemas de informação do oponente.
c) ESPAÇO CIBERNÉTICO – espaço virtual composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas e/ou armazenadas.
d) GUERRA CIBERNÉTICA – corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C2 do adversário, 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 Sist Info. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcionado à dependência do oponente em relação às TIC.

3 GUERRA CIBERNÉTICAS NAS OPERAÇÕES DEFENSIVAS

As ações defensivas buscam evitar ou minimizar ataques cibernéticos lançados pelo inimigo, protegendo a informação, e restaurar rapidamente os danos e limitações oriundas desses ataques, impingidas às capacidades cibernéticas, garantindo a utilização do Espaço Cibernético.

Conforme o Manual EB 70-MC-10.232, nas operações defensivas prevalecem as ações de proteção cibernética. A manutenção dessas ações em relação aos sistemas de informação em uma operação costuma ser crítica. A G Ciber é fundamental em uma defesa móvel em razão dos seguintes fatores:

a) Intenso fluxo da informação;
b) Rapidez na tomada de decisões e na difusão das ordens; e
c) Coordenação de todas as funções de combate em tempo e espaço.

3.1 Brasil na Guerra Cibernética

A crescente presença dos Estados no espaço cibernético e as atividades dos atores não estatais, incluindo entidades comerciais, criminosos cibernéticos e grupos terroristas, tornam o ciberespaço um ambiente cada vez mais complexo e vulnerável. Essa vulnerabilidade tem influenciado Políticas Estatais para garantir a proteção das estruturas nacionais. O Brasil estabeleceu na Política Nacional de Defesa (PND), na Estratégia Nacional de Defesa (END) e na Política Cibernética de Defesa (PCD) os parâmetros de atuação necessários à preparação do País para atuar no domínio cibernético.

A END define o Setor Cibernético como um dos três setores estratégicos nacionais, sendo uma de suas prioridades a implantação do Comando de Defesa Cibernética, que a partir de dezembro de 2012 passou a coordenar o Sistema Brasileiro de Defesa Cibernético (SBDC).

O SBDC está dividido em três níveis de atuação: político, estratégico e operacional e tem como finalidade atender os objetivos da END referentes à defesa cibernética, coordenando os diversos órgãos do Estado no que se refere a esse tema. A Figura 1 apresenta a distribuição das instituições pelo SBDC:

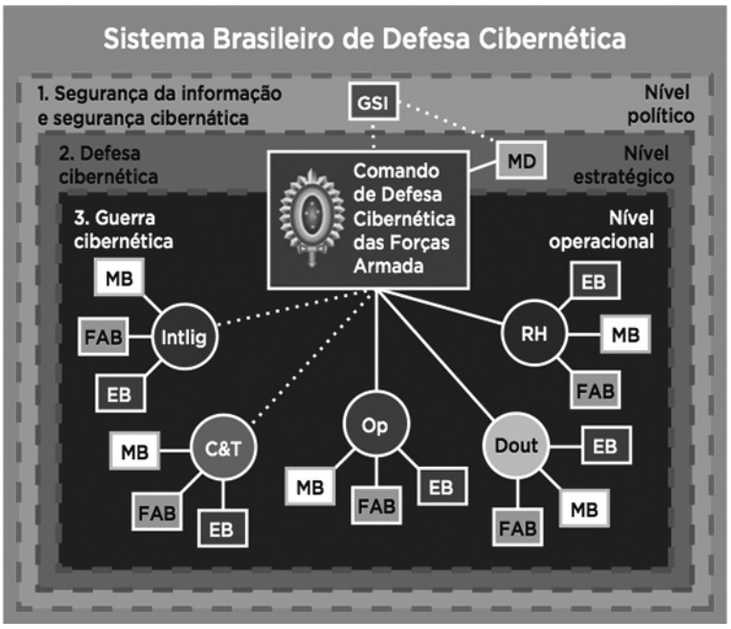

Figura 1 – Sistema Brasileiro de Defesa CIbernética

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) é o coordenador da segurança de informação e comunicação (SIC) e cibernética (SC) zelando pela segurança dos sistemas afetos à infraestrutura nacional de energia (eletricidade, petróleo e gás), o sistema financeiro e a infraestrutura social (transportes, abastecimento e outros serviços públicos).

O GSI/PR age de forma coordenada com o MD que é o coordenador da defesa cibernética, a nível estratégico, e da guerra cibernética, a nível tático/operacional. O Comando de Defesa Cibernética das Forças Armadas, dentro da estrutura do SBDC, exerce papel de assessoria executiva ao MD e ao GSI/ PR sendo responsável pela parte executiva das ações de defesa cibernética, a nível estratégico, e pela coordenação das três forças armadas, Marinha, Exército e Aeronáutica, à nível tático/operacional, no que se refere aos aspectos logísticos, operacionais, doutrinários, de CT&I e recursos humanos afetos à guerra cibernética propriamente dita. A coordenação do SBDC a nível nacional cabe ao Exército Brasileiro, que é responsável pelo Comando de Defesa Cibernética das Forças Armadas.

No Brasil, a Guerra Cibernética prioriza a segurança de informação e comunicação, segurança cibernética e defesa dos ativos de informação da Administração Pública Federal. O MD, por meio da END e da PCD, mostra excessiva preocupação com os níveis político e estratégico do SBDC, deixando a desejar, porém, no que diz respeito à Defesa Cibernética de nível tático-operacional, que é deixada a critério de cada força singular, e à Guerra Cibernética propriamente dita, parecendo menosprezar os efeitos de ataques cibernéticos fora do âmbito das estruturas críticas nacionais.

3.2 Defesa Cibernética nos Países Desenvolvidos

A ameaça do futuro para os países desenvolvidos, como a Suíça, virá dos vírus e vermes digitais. Para piorar ainda mais a situação, os vermes digitais podem se autorreproduzir e infectar redes inteiras, sem necessariamente precisar de um meio físico, como um disco rígido, podendo inclusive atacar infraestruturas industriais.

A Suíça precisa se proteger de incidentes no futuro, como o que atingiu o Ministério das Relações Exteriores da Suíça (DFAE), em outubro de 2009. Um ataque feito com um programa malicioso que permitiu que hackers invadissem a infraestrutura do DFAE e tivessem acesso a várias informações confidenciais.

O Ministério Público Federal continua investigando o caso para saber quem estava por trás deste ato de espionagem. A única certeza até o momento é que ele serviu como exemplo das ameaças que o país deve enfrentar no futuro e do nível da segurança contra esses ataques. Um balanço da situação com o novo chefe da defesa cibernética e seu suplente, Gerald Verner.

O projeto de defesa cibernética na Suíça está sob os auspícios do Ministério da Defesa, da Proteção Civil e dos Esportes (DDPS). A defesa cibernética abrange cinco áreas:

a) Direção: Preparar a Suíça para administrar os riscos de ataques cibernéticos e uma eventual crise.
b) Operações defensivas: Consistem no acompanhamento da situação, reforço dos sistemas e defesa deles em caso de ataque, especialmente entrando nos sistemas adversários.
c) Desenvolvimento contínuo: Para tomar as decisões corretas em caso de ataque, é necessário antecipar as ameaças.
d) Desenvolvimento de regras: As regras devem ser claras para definir até onde podemos ir na defesa cibernética nacional e internacional.
e) Treinamento: É muito importante, porque diversos estudos demonstram que o elo mais fraco é o homem e o sistema mais seguro pode ser sempre atacado por dentro. Assim, devemos sensibilizar, educar e treinar os diferentes usuários.

4 A FORÇA TERRESTRE COMPONENTE EM OPERAÇÕES OFENSIVAS

As operações ofensivas, no tocante à Guerra Cibernética, devido à complexidade das redes e sua rápida adaptação ao desenvolvimento das ações, exigem um minucioso planejamento. Para ações cibernéticas serão empregados todos os recursos, com o objetivo de criar soluções alternativas para o cumprimento da missão. Crescem, então, de importância as ações de Ataque e Exploração Cibernética. Alinhado aos fogos e junto com a GUERRA ELETRÔNICA, deve-se elaborar uma lista de alvos cibernéticos (LIA Ciber) e uma lista priorizada de alvos cibernéticos (LIPA Ciber).

As operações em Amplo Espectro têm por característica a combinação (simultânea ou sucessiva) de diferentes atitudes, Ofensivas, Defensivas ou de Cooperação e Coordenação com Agências, com máxima integração entre as forças e com outras agências, tudo isso aplicado em uma escala variável de violência. Portanto, torna-se nítido que a flexibilidade de uma FTC é fator preponderante para o sucesso de sua missão, haja vista a gama de ações a serem desencadeadas em prol dos diversos tipos de operações.

A Operação Ofensiva (Op Ofs) é caracterizada, de acordo com o Manual de

Campanha Operações Ofensivas e Defensivas (EB-70-MC-10.202), por uma "ação decisiva de emprego da força militar no campo de batalha, para impor a nossa vontade sobre o inimigo que se concentra para o combate de alta intensidade, representando o melhor caminho para se obter a vitória". Nota-se que é o tipo de operação que deve ser privilegiada, pois sempre trará, de acordo com a doutrina, os melhores resultados para quem as tiver executando.

Verifica-se que os objetivos das Op Ofs são extremamente variados e demandam uma ampla diversidade de ações, desde aquelas mais voltadas para um caráter bélico até as direcionadas para dissimulação. Dessa maneira, já é possível visualizar que a Guerra Cibernética pode contribuir com diferentes intensidades sobre esse tipo de operação, considerada prioritária sob a ótica doutrinária.

4.1 Estratégias de Guerra Cibernética ao redor do mundo

A importância da Guerra Cibernética percebe-se desde o início do corrente século, devido aos ataques que puderam ser identificados em conflitos localizados ao redor do mundo e pelas ações que têm sido realizadas pela maioria dos países para se prepararem para fazer face a esta nova e muito perigosa ameaça.

Veremos então algumas das principais ações ofensivas de Guerra Cibernética e seus efeitos no contexto dos conflitos em que estavam enquadradas, assim como as principais ações estratégicas adotadas por alguns países para o desenvolvimento da área cibernética em suas sociedades.

4.1.1 Estados Unidos da América

Devido ao seu pioneirismo em relação à Internet e seu alto nível de desenvolvimento tecnológico, os Estados Unidos da América (EUA) têm buscado protagonismo em relação à atuação no ambiente cibernético.

Principalmente a partir da década de 1990, com a popularização da Internet, as preocupações do Departamento de Defesa Americano (*DoD*) com as vulnerabilidades que poderiam ameaçar os EUA a partir da conexão de suas redes com a Internet aumentaram sensivelmente. No ano de 1995, o General da Força Aérea Albert J. Edmonds, então diretor da Agência de Defesa de Sistemas de Informação (*Defense Information Systems Agency* – DISA) ao proferir uma palestra na Universidade de Harvard alertou que as redes de computadores dos EUA eram vulneráveis a ataques remotos (USA, 2018a).

No final da década de 1990, a preocupação com a defesa dessas redes era da própria DISA, por intermédio da Força Tarefa Conjunta de Defesa de Redes de Computadores (*Joint Task Computer Network Defense – JTF-CND*), primeira organização do DoD com autoridade para supervisionar e dirigir operações nas redes. Essa Força Tarefa se transformou, no final de 1999, na Força Tarefa de Operações em Redes de Computadores (*Joint Task Computer Operations – JTF-CNO*) (USA, 2018). Após várias evoluções em decorrência dos anos e com a evolução da internet, no ano de 2017, o Presidente Donald Trump decidiu aceitar a recomendação do Secretário de Defesa James Mattis e elevar o *United States Cyber Command* (USCYBERCOM), a um comando combatente unificado responsável pelas operações cibernéticas, não mais estando subordinado ao *United States Strategic Command* (USSTRATCOM). A mudança se concretizou em maio de 2018. (USA, 2018b). O USCYBERCOM executa as suas atividades por intermédio das unidades cibernéticas componentes existentes nas diversas Forças Armadas dos EUA, a saber (apud Bernat Júnior, 2012, p. 16):

O DoD estabeleceu, no ano de 2011, cinco iniciativas estratégicas que ainda estão sendo praticadas dentro dessa nova conformação do USSCYBERCOM:

a) Primeira iniciativa estratégica: o DoD irá tratar o ciberespaço como um domínio operacional para organizar, treinar e equipar, de forma que seja possível ao DoD, aproveitar-se de todas as suas vantagens potenciais.

b) Segunda iniciativa estratégica: o DoD irá empregar novos conceitos operacionais de defesa para defender as suas redes e sistemas.
c) Terceira iniciativa estratégica: o DoD irá realizar parcerias com outras agências do governo americano e com a iniciativa privada, que permitam estabelecer uma estratégia completa de segurança cibernética.
d) Quarta iniciativa estratégica: o DoD irá estreitar os laços com os aliados americanos e parceiros internacionais de forma a aumentar a cibersegurança coletiva.
e) Quinta iniciativa estratégica: o DoD irá trabalhar para diminuir a ingenuidade de danação em termos de atuação nos ambientes cibernéticos, na tentativa de gerar uma força de trabalho cibernético excepcional, capaz de produzir com rapidez inovações tecnológicas na área em questão.

Das estratégias citadas, é preciso destacar as grandes vantagens americanas devido às possibilidades de parcerias com a iniciativa privada. Destaca-se ainda a identificação, na quinta iniciativa, da necessidade de desenvolver no povo americano como um todo os conhecimentos necessários à utilização correta e segura dos serviços disponíveis e cada vez mais comuns no espaço cibernético, principalmente a Internet.

A partir dessa declaração, é possível concluir que o governo americano identifica que sem essa conscientização, todos os esforços do DoD e seus órgãos ligados à defesa cibernética ficarão seriamente comprometidos, principalmente devido às vulnerabilidades que podem surgir do uso da Internet sem os cuidados mínimos com a segurança pelos usuários americanos em suas atividades, sejam elas profissionais ou sociais.

4.1.2 Rússia

A Rússia surgiu nos últimos anos como um dos países que mais tem sido associado a ações de Guerra Cibernética no mundo. Uma série de ações a ela atribuídas em diversos conflitos demonstram que o gigante russo tem conseguido se adaptar à nova era e entender as potencialidades deste novo tipo de guerra.

A consequência imediata foi uma série de conflitos com ex-repúblicas soviéticas, nos quais a Rússia empregou não apenas as suas forças armadas convencionais, mas principalmente utilizou diversas ações de Guerra Cibernética que mostraram ao mundo toda a sua eficiência e potencial.

O primeiro país a sofrer tais ataques foi a Estônia, que havia se tornado independente da URSS em 1989. O conflito com a Rússia se iniciou em 2007, quando por pressões populares, o legislativo da Estônia aprovou a Lei das Estruturas Proibidas, que determinava que qualquer símbolo que fizesse menção às cinco décadas de ocupação soviética fosse derrubado. Isso incluía a estátua de um soldado de bronze do Exército Vermelho, situada na capital da Estônia, e erguida para lembrar o sacrifício feito pelo Exército Soviético para libertar a Europa dos nazistas na II Guerra mundial.

Além do simbolismo existente na estátua, havia soldados soviéticos enterrados ao redor da mesma, o que provocou um forte posicionamento de Moscou declarando que derrubar o Soldado de Bronze seria difamar os soldados soviéticos mortos. Na tentativa de contornar a crise, o presidente estoniano vetou a lei, provocando um aumento das pressões internas, fosse de cidadãos estonianos favoráveis à retirada da estátua, fosse de cidadãos russos moradores da região, que defendiam a sua permanência.

Após a eclosão de um conflito entre manifestantes russos e estonianos em torno da derrubada da estátua, naquela que ficou conhecida como Noite de Bronze, as autoridades estonianas moveram a estátua numa tentativa de acalmar o conflito.

Logo após, a Estônia foi vítima de um ataque cibernético até então sem precedentes. O país sofreu um ataque distribuído de negação de serviço (DDoS) que levaram ao colapso os principais servidores do país. Este é um tipo de ataque em que milhares de computadores são mobilizados para enviar pings a vários alvos na Internet.

Um "*ping*" é um comando para que um computador envie um pacote padronizado a outro computador específico, por meio do seu endereço IP. Neste tipo de ataque, os milhares de computadores infectados enviam simultaneamente os pacotes "ping" a um alvo específico, inundando-os e fazendo com que não consigam responder à demanda provocada e parem de funcionar corretamente.

Os computadores atacantes são chamados de *botnet*, uma rede robótica de computadores "zumbis" controlados remotamente. Os zumbis atacam seguindo instruções que são acionadas sem o conhecimento de seus proprietários. Esses computadores muitas vezes estão infectados há semanas ou mesmo meses, apenas esperando um comando do seu computador "mestre" para que iniciem o ataque.

O ataque de DDoS à Estônia foi sem precedentes até aquele momento porque normalmente, servidores que sofriam este tipo de ataque eram atingidos por pouco tempo, dias no máximo. No caso da Estônia porém, o ataque durou semanas e atingia centenas de sites importantes do país, de forma ininterrupta, impedindo-os de voltar a funcionar corretamente.

Durante o ataque, foram atingidos servidores que apoiavam parte da rede telefônica da Estônia, do sistema de cartões de crédito e do serviço de diretório da Internet, do Hansapank, que era o maior banco do país, afetando o comércio e os serviços de comunicação, provocando caos e prejuízo ao país.

A Estônia solicitou apoio à OTAN, que mobilizou uma equipe para apoiar o país, mas os ataques continuaram, já que os computadores zumbis aparentemente se adaptaram, talvez reprogramados pelo seu "mestre". Especialistas rastrearam os "pings" e alegaram que as máquinas de controle finais estavam na Rússia, e que o código do programa havia sido escrito em alfabeto cirílico. O país negou com veemência qualquer participação nos ataques, mas se recusou a identificar os autores que se alegava estarem em seu território. Pressionado, o governo russo admitiu que os ataques poderiam ter partido de nacionalistas russos em seu território, inconformados com os acontecimentos na Estônia e sua "hostilidade contra o povo russo". Mas negou que tais nacionalistas fossem patrocinados ou mesmo incentivados pelo governo russo.

O ataque cibernético levou a OTAN a criar, em 2008, um centro de defesa cibernética a poucos quilômetros do local onde o soldado de bronze gigante originalmente ficava, onde há agora um pequeno e agradável bosque.

5 CONSIDERAÇÕES FINAIS

O poder de combate de uma Força Terrestre Componente no seu emprego nas operações militares ofensivas e defensivas, hodiernamente, não se mensura mais somente em seu poderio bélico e militar, mas sim em sua capacidade de obter, explorar, controlar, atacar e defender um Sistema de Tecnologia da Informação e Comunicações do inimigo. Um ataque cibernético pode ser considerado como uso da força de uma Nação mesmo quando não destrua diretamente o adversário, apenas desabilitando ou roubando informações do alvo em questão pode ser muito mais danoso que destruí-lo propriamente.

Face a um ambiente situacional cada vez mais conectado, é notória a urgência e a necessidade de uma Nação em se criar, desenvolver, gerir e proteger um sistema de defesa cibernética seja por parte de civis, por parte de militares ou ambos, visando seu emprego frente a possíveis ataques cibernéticos como os que ocorreram na Estônia pela Rússia, nos EUA e até mesmo no Brasil. Nesse diapasão, o Brasil criou através do Ministério da Defesa o seu Sistema de Defesa Cibernética e Guerra Eletrônica, o qual vem se desenvolvendo e sendo empregado nas diversas operações de Coordenação e Cooperação com Agências, o que tem gerado resultados positivos e melhorias em todo o sistema.

O emprego da guerra cibernética nas operações militares transcendem as fron-

teiras físicas e se estabelecem no mundo digital, no campo de batalha cibernética, onde não existe um sistema totalmente seguro cabendo ao Exército Brasileiro como responsável pelo Comando de Defesa Cibernética das Forças Armadas manter-se preparado e aperfeiçoar-se continuamente no uso do amplo espectro, a fim de manter a integridade das fronteiras e a segurança da informação e comunicações para emprego da capacidade militar terrestre cibernética.

REFERÊNCIAS

AVELAR, José Ricardo Cabral. **A Guerra Cibernética e seus desafios para o Brasil**. 2018. 74 f. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2018.

BRASIL**. Exército. Estado-Maior. Guerra Cibernética. 1. ed. Brasília, DF. 2017.**

_____. Exército. Estado-Maior. **Doutrina Militar Terrestre**. 1ª. ed. Brasília, DF. 2014a.

_____. Exército. Estado-Maior. **Força Terrestre Componente**. 1ª. ed. Brasília, DF. 2014.

_____. Exército. Estado-Maior. **Força Terrestre Componente nas Operações**. 1ª. ed. Brasília, DF. 2014.

_____. Exército. Estado-Maior. **Operações**. 5. ed. Brasília, DF. 2017.

_____. Exército. Estado-Maior. **Operações Ofensivas e Defensivas**. 1. ed. Brasília, DF. 2017.

_____. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. 1. ed. Brasília, DF. 2014.

_____. Ministério da Defesa. **Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas**. 3. ed. Brasília, DF. 2008.

EUA. Cyber Command. **Histórico da Defesa Cibernética dos EUA**. Disponível em <https://www.cybercom.mil/About/History/> Acesso em 17 de novembro de 2019.

EUA. Department of Defense. **Departamento de Defesa inicia processo para elevar o Cyber Comando dos EUA a um Comando Unificado**. Disponível em <https://dod.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/. Acesso em 17 de novembro de 2019.

GAZETA DO POVO. **Falha grave em segurança do Wi-Fi deixa redes à mercê de ataques**. Disponível em: <https://www.gazetadopovo.com.br/economia/nova-economia/falha-grave-em-seguranca-do-wi-fi-deixa-redes-a-merce-de-ataques-39gs7cb1o64n6cn3p5pf4lcej/> Acesso em: 16 de novembro de 2019.

GAZETA DO POVO. **Hackers norte-coreanos roubaram táticas de guerra dos EUA e da Coreia do Sul**. Disponível em: <http://www.gazetadopovo.com.br/mundo/hackers-norte-coreanos-roubaram-taticas-de-guerra-dos-eua-e-da-coreia-do-sul-d4jcdi77i3tr0lwviz1aen8lz> Acesso em: 16 de novembro de 2019.

NETO, Samuel Bombassaro. **A atuação da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente em operações ofensivas**. 2018. 55 f. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2018.