ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

Cel COM **SÉRGIO** ALEXANDRE SALDANHA LEITE REZENDE DE **MATTOS**

As Comunicações no Combate Moderno: "Arma de Apoio ao Combate ou Arma decisiva para a resolução dos Conflitos?" Uma mudança de paradigma baseada em novas tecnologias integradas

Rio de Janeiro
2021

Cel COM **SÉRGIO** ALEXANDRE SALDANHA LEITE REZENDE DE **MATTOS**

As Comunicações no Combate Moderno: “Arma de Apoio ao Combate ou Arma decisiva para a resolução dos Conflitos?” Uma mudança de paradigma baseada em novas tecnologias integradas

Policy Paper apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Política, Estratégia e Alta Administração Militar.

Orientador: Cel R/1 Art WANDERLEY MONTEAGUDO RASGA JUNIOR

Rio de Janeiro
2021

M444c Mattos, Sérgio Alexandre Saldanha Leite Rezende de.

As Comunicações no Combate Moderno: “Arma de Apoio ao Combate ou Arma decisiva para a resolução dos Conflitos?” Uma mudança de paradigma baseada em novas tecnologias integradas / Sérgio Alexandre Saldanha Leite Rezende de Mattos. ─ 2021.
41 f. : il. ; 30 cm.

Orientação: Wanderlei Monteagudo Rasga Júnior
Policy Paper (Especialização em Política, Estratégia e Alta Administração Militar) ─ Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2021.
Bibliografia: f. 37-41

1. NOVAS TECNOLOGIAS. 2. COMUNICAÇÕES 3. GUERRA ELETRÔNICA. 4. GUERRA CIBERNÉTICA. 5. COMANDO E CONTROLE. I. Título.

Cel COM **SÉRGIO** ALEXANDRE SALDANHA LEITE REZENDE DE **MATTOS**

As Comunicações no Combate Moderno: “Arma de Apoio ao Combate ou Arma decisiva para a resolução dos Conflitos?” Uma mudança de paradigma baseada em novas tecnologias integradas

Policy Paper apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Política, Estratégia e Alta Administração Militar.

Aprovado em _____ de _____ de 2021.

COMISSÃO AVALIADORA

_____
WANDERLEY MONTEAGUDO RASGA JUNIOR - Cel Art R1– Presidente /Orientador
Escola de Comando e Estado-Maior do Exército

_____
LUIS HENRIQUE PEDROZA MENDES – Cel R1 Com – Membro
Escola de Comando e Estado-Maior do Exército

_____
SÉRGIO WILTON LOPES DE BARROS – Cel R1 Inf – Membro
Escola de Comando e Estado-Maior do Exército

RESUMO EXECUTIVO

A Especialização de Comunicações foi criada, no Exército Brasileiro, na década de 1960 com o objetivo de instalar, explorar e manter os sistemas de comunicações, em todos os níveis, em apoio as Operações. Este trabalho tem sido desenvolvido de forma silente por décadas. Recentemente, com o advento de novas tecnologias e da modernização dos equipamentos, as Comunicações tem adquirido uma importância cada vez maior para o estabelecimento dos sistemas de forma eficaz e dinâmica, em todos os níveis, assumindo muitas vezes um papel de protagonista na resolução de conflitos. Tal fato ocorre pelo desenvolvimento de novas tecnologias (satelital, microondas, entre outras) e pelo aparecimento, aprimoramento e integração de duas novas vertentes do Combate Moderno: a Guerra Eletrônica e a Guerra Cibernética. Tais vertentes têm levado o Comando e Controle a uma posição de destaque em todas as Operações e permitido aos Comandantes a tomada de decisões que, muitas vezes, neutralizam intenções hostis mesmo antes do emprego de tropas. Este oficial possui o Curso de Guerra Eletrônica e quase 30 anos de experiência na Arma de Comunicações, podendo atestar as mudanças ocorridas ao longo do tempo e o crescimento da importância do emprego do Comando e Controle para a resolução de conflitos, principalmente após o aparecimento da Guerra Eletrônica e da Guerra Cibernética. Este trabalho buscará demonstrar a nova realidade da Arma de Comunicações nos dias atuais.

Palavras-chave: NOVAS TECNOLOGIAS. COMUNICAÇÕES. GUERRA ELETRÔNICA. GUERRA CIBERNÉTICA. COMANDO E CONTROLE.

EXECUTIVE SUMMARY

The Communications Specialization was created in the Brazilian Army in the 1960s with the objective of installing, exploring and maintaining communications systems, at all levels, in support of Operations. This work has been developed from silent way for decades. Recently, with the advent of new technologies and the modernization of equipment, Comunications has gained increasing importance for the establishment of systems in an effective and dynamic way, at all levels, often playing a leading role in conflict resolution. This fact occurs due to the development of new technologies (satelite, microwave, among others) and to the appearance, improvement and cyberware. Such aspects have taken Command and Control to a prominent position in all Operations and allowed Commanders to take decisions that often neutralize hostile intentions even before the use of troops. This officer has an eletronic warfare course and nearly 30 years of experience in the army, as a communications specialist, and can attest the changes that occurred over time and the growing importance of using Command and Control to resolve conflicts, especially after the appearance of eletronic warfare and cyberwarfare. This work will seek to demonstrate the new reality of communications today.

Keywords: NEW TECHNOLOGIES. COMMUNICATIONS. ELECTRONIC WAR. CYBER WAR. COMMAND AND CONTROL.

LISTA DE ABREVIATURAS E SIGLAS

C Mil A	Comandos Militares de Área
Cmt	Comandante
C²	Comando e Controle
DCT	Departamento de Ciência e Tecnologia
EB	Exército Brasileiro
ED	Estratégia de Defesa
EMD	Estratégia Militar de Defesa
EME	Estado-Maior do Exército
END	Estratégia Nacional de Defesa
F Ter	Força Terrestre
FA	Forças Armadas
GM	Guerra Mundial
HE	Hipótese de Emprego
MD	Ministério da Defesa
ODS	Órgão de Direção Geral
OEE	Objetivo Estratégico do Exército
OM	Organização Militar
PBC	Planejamento Baseado em Capacidades
PEEx	Plano Estratégico do Exército
PND	Política Nacional de Defesa
SEC²Ex	Sistema Estratégico de Comando e Controle
SC²FTer	Sistema de Comando e Controle da Força Terrestre
SIPLEX	Sistema de Planejamento Estratégico do Exército
SIPLOM	Sistema de Planejamento Operacional Militar
SISMC2	Sistema Militar de Comando e Controle
SEC	Sistema Estratégico de Comunicações
Sis Tat C	Sistema Tático de Comunicações
SNT	Sistema Nacional de Telecomunicações
TI	Tecnologia de Informação
TIC	Tecnologia de Informação e Comunicações

SUMÁRIO

1 INTRODUÇÃO

As primeiras formas de comunicação ocorreram, entre pessoas, da maneira mais rudimentar, até a formação de palavras e frases.

Em um segundo momento, surgiu a necessidade de aumentar as distâncias, para se transmitir informações e mensagens. Para isso, foram usados sistemas sonoros, como tambores e sistemas visuais, como bandeirolas e fumaça.

As primeiras invenções de comunicações provocaram mudanças sobre a cultura dos povos, modificando perspectivas sociais, econômicas, políticas e científicas.

Samuel Morse construiu o primeiro aparelho telegráfico, em 1830, estabelecendo os princípios do código de pontos, traços e intervalos, de acordo com a presença ou a ausência de impulsos elétricos, criando o principal meio de ligação do século XIX.

O escocês Alexander Graham Bell patenteou, em 1876, a invenção do telefone, após realizar o estudo que permitia a transmissão de sons, por meio de eletricidade e, alguns anos depois, em 1885, com a criação da Companhia de Telefones e Telégrafos, iniciaram-se as operações de comunicações, de longa distância.

Em 1932, Guglielmo Marconi inovou com a transmissão de sinais sem fio, implementando o primeiro link terrestre de telefonia em ondas curtas e, em 1935, ao adaptar esses princípios para o mar, demonstrou os princípios do radar.

A história das Comunicações no EB está diretamente relacionada com a criação da Escola de Comunicações, em julho de 1921. Com base nos acontecimentos da I GM (1914/1918), observou-se a necessidade de reestruturar diversos setores nos exércitos, levando-se em consideração a velocidade das ações e de deslocamento das tropas.

As I e II GM colaboraram para o desenvolvimento de sistemas de comunicações, por fio, rádios e até mesmo a criação dos primeiros computadores, com objetivos militares.

Sob a orientação da Missão Militar Francesa, foi criado e consolidado o Centro de Instrução e Transmissão (CIT), embrião da 1ª Cia Transmissões, responsável por todas as ligações realizadas, nos campos de Batalha da Europa, durante a II GM.

As vitórias alcançadas pela Força Expedicionária Brasileira (FEB) tiveram uma influência considerada fundamental pelo Comandante da 1ª DIE, o Gen Div Mascarenhas de Moraes, nos seguintes termos:

> Nota de Comando Nº 8: *"V-Exército - IV-Corpo - 1ª DIE - ESTADO-MAIOR - 1ª Seção Itália, 3 fev 1945".* ***ÀS TRANSMISSÕES DA FEB***
> *Em nenhuma ocasião, o Comandante da FEB deixou de transmitir as suas ordens ou receber informação dos escalões subordinados, por falta de meios. De dia ou de noite, em situações de calma ou de combate, as transmissões têm estado à altura de sua importante missão.*
> ***JOÃO BATISTA MASCARENHAS DE MORAIS*** *– Gen Div, "Cmt 1ª DIE".*

Após o fim da II GM, o Brasil passou a utilizar equipamentos de comunicações empregados na Guerra, de origem americana, e a instrução militar passou a ser ministrada, com base na Comissão Militar Mista Brasil-EUA.

Por meio da Lei nº 2.851, de 25 de agosto de 1956, foi criada a Arma de Comunicações, e em 1963, o Marechal Cândido Mariano da Silva Rondon foi designado "Patrono da Arma de Comunicações do Exército Brasileiro".

Muitas tecnologias de Comunicações foram oriundas da disputa entre EUA e URSS, por ocasião da "Guerra Fria", onde os sistemas de comunicações foram automatizados e alimentados, com uma série de componentes eletrônicos.

Destaca-se, ainda, o aparecimento da rede mundial de computadores: "a Internet", capaz de estreitar distâncias e introduzir novas formas de tecnologia, em apoio aos combates modernos, também conhecidos como conflitos de 5ª geração.

Tais tecnologias impulsionam o sistema de comunicações tradicional, com novos equipamentos, que permitem a exploração do ambiente eletromagnético e do ciberespaço, com sistemas que integram novas capacidades conhecidas como Guerra Eletrônica e Guerra Cibernética, respectivamente. O Espectro eletromagnético, se tornou um novo campo de batalha, decisivo, antes mesmo do primeiro disparo de uma arma de fogo.

Após o breve histórico sobre as Comunicações e o seu desenvolvimento tecnológico, é importante esclarecer que este trabalho foi desenvolvido com o objetivo de verificar as novas perspectivas da Arma, num ambiente volátil, incerto, complexo e ambíguo (VUCA, sigla em inglês), existente nos combates modernos.

A Arma de Comunicações é conhecida, no Exército Brasileiro (EB), como a Arma do Comando pois proporciona, aos Comandantes em todos os escalões, a formação de uma consciência situacional completa e atualizada, face aos oponentes, preservando a integridade das suas ações e o desenvolvimento das Operações.

Desde a sua criação é considerada uma Arma de apoio ao combate; este trabalho buscará demonstrar que a mesma adquiriu um novo “status”, passando a ser decisiva na resolução dos conflitos.

2 METODOLOGIA

O presente trabalho seguirá a metodologia apresentada, a seguir.

2.1 PROBLEMA

A Arma de Comunicações tem evoluído muito, nas últimas décadas, pelo aparecimento de novas tecnologias impostas pelas novas vertentes do Combate Moderno: mencionam-se a Guerra Eletrônica e a Guerra Cibernética.

Entretanto, ainda não está clara a importância da Arma do Comando e o seu papel preponderante para a resolução dos conflitos atuais.

Assim sendo, surge a situação-problema da pesquisa: as Comunicações deixaram de ser uma arma de apoio, para se tornarem uma arma decisiva para a resolução dos conflitos?

2.2 OBJETIVOS

2.2.1 Objetivo Geral:

- Demonstrar que a Arma de Comunicações assumiu um novo papel no Combate Moderno, pelo uso de novas tecnologias integradas e pelo surgimento da Guerra Eletrônica e da Guerra Cibernética, deixando de ser uma Arma de Apoio e passando a ser decisiva, na resolução dos conflitos.

2.2.2 Objetivos específicos:

- Apresentar a evolução da Arma de Comunicações;
- Apresentar os principais conceitos sobre a função Comando e Controle;
- Apresentar conceitos de Guerra Eletrônica e Guerra Cibernética;
- Apresentar as possibilidades de integração da Guerra Eletrônica e da Guerra Cibernética, para a resolução de conflitos e fortalecimento da Arma de Comunicações;
- Demonstrar a necessidade de mudança de paradigma, quanto à importância da Arma do Comando, na resolução dos conflitos modernos.

2.3 DELIMITAÇÃO DO ESTUDO

Este trabalho limitar-se-á a realizar um estudo sobre a evolução das comunicações, sendo apresentados casos históricos, que demonstram que a Arma de Rondon possui um novo “status” no Combate moderno, sendo decisiva para a solução dos conflitos.

2.4 RELEVÂNCIA DO ESTUDO

Esta pesquisa contribuirá com o EB, na medida em que poderá cooperar com a evolução da doutrina de planejamento da Arma de Comunicações, ferramenta fundamental do C² do Exército, apresentando a necessidade de mudar a visão da força, quanto a sua relevância, no contexto atual, para a obtenção do sucesso, nos combates modernos de 5ª Geração.

2.5 METODOLOGIA

A pesquisa proposta neste trabalho buscou, por meio do uso de diversas fontes de consulta (manuais, artigos, entre outras); e observando situações reais ocorridas nos últimos anons; tentar demonstrar a necessidade de mudança de paradigma do emprego Arma de Comunicações, como uma ferramenta de resolução dos conflitos recentes, com função estratégica, na mão dos comandantes, em todos os níveis.

Seguindo a taxionomia de Vergara (2008), a pesquisa será explicativa, bibliográfica e documental. Explicativa, porque o autor buscará tornar o assunto o menos complexo possível; bibliográfica, porque terá a sua fundamentação teórico-metodológica calcada na investigação dos assuntos abordados e na exploração do conhecimento disponível em livros, manuais, artigos e redes eletrônicas de acesso livre ao público; e documental, porque valer-se-á de documentos, relatórios e regulamentos não disponíveis para consultas públicas.

Os dados levantados serão tratados pela análise do conteúdo que, segundo Vergara (2008), é “uma técnica, que visa identificar o que está sendo dito, a respeito de determinado tema”.

3 REVISÃO DA LITERATURA

Com a finalidade de compreender o assunto pesquisado, realizou-se uma revisão da literatura (artigos e publicações militares) relacionada com o tema.

3.1 O AMBIENTE VUCA

O Manual EB20-MF-10.101 define que os conflitos atuais se apresentam com novas características e tendências, em um ambiente redefinido por extensa rede de sensores e de fluxo de dados, centrada no comandante; proporcionam vantagens decisivas a quem melhor integrar, analisar, difundir e utilizar, com oportunidade, as informações relevantes.

O mundo do século XXI não é mais o mesmo. Com o advento da Revolução técnico-científica, as distâncias foram encurtadas e os eventos, que ocorrem do outro lado do planeta, impactam, instantaneamente, a vida das pessoas.

Tal situação não é diferente, no que diz respeito ao emprego das forças armadas; neste caso, o Comandante, em todos os níveis, precisa acompanhar todas as ações, com o máximo de informações, para consolidar uma consciência situacional plena, que permita a tomada de uma decisão eficaz.

Os exércitos devem ser dotados de características, que minimizem as dificuldades encontradas em um ambiente "volátil, incerto, complexo e ambíguo" (acrônimo em inglês VUCA – "*volatility, uncertainty, complexity and ambiguity"). Este* conceito surgiu, na década de 1990, nas Forças Armadas dos Estados Unidos.

Figura 1 – Mundo VUCA

Site https://professorannibal.com.br/2018/03/13/identificando-e-desenvolvendo-oportunidades-em-um-mundo-vuca/

A PND/2016 define que o cenário internacional é caracterizado por assimetrias de poder, gerando tensões e instabilidades, que contribuem para o surgimento de grupos insurgentes e de organizações terroristas ou criminosas, tendentes a incrementar a guerra irregular.

A ocorrência de conflitos generalizados, entre Estados, teve reduzida a sua incidência e renovaram-se aqueles de caráter étnico e religioso, exacerbando-se os

nacionalismos e fragmentando-se os Estados, cenário propício para o desenvolvimento da denominada “guerra híbrida”.

A END/2016 destaca que as relações internacionais se mantêm instáveis com desdobramentos, por vezes, imprevisíveis. Assim, conforme defendido pelo Barão do Rio Branco, o Brasil tem a consciência de que “nenhum Estado pode ser pacífico sem ser forte", de modo que o crescente desenvolvimento do País deve ser acompanhado pelo adequado preparo de sua defesa.

O EB não está alheio às características do mundo VUCA, que causa o achatamento dos níveis de planejamento e de condução dos conflitos. Sem um C² eficaz, é impossível obter uma consciência situacional adequada para o comandante considerado.

3.2 A GUERRA HÍBRIDA

As mudanças experimentadas pelas sociedades, com reflexos na forma de fazer política e o surgimento de nova configuração geopolítica conduzem a horizontes incertos e complexos, para o planejamento da Defesa da Pátria.

Tais mudanças alteram as relações de poder, provocando instabilidades e incertezas e suscitam o aparecimento de conflitos locais e regionais, com a inserção de novos atores estatais e não estatais, no contexto dos conflitos (BRASIL, 2013).

Nessa esteira, surge a definição de Guerra Híbrida. Segundo a PND 2016, ela define os novos conflitos do século XXI, frequentemente, chamados de “conflitos do futuro”, onde ações de combate convencional são permeadas, no tempo e no espaço, por operações de natureza irregular, de guerra cibernética e de operações de informação, dentre outras, com atores estatais e não estatais, no ambiente real e informacional, incluindo as redes sociais.

Figura 2 – Representação da Guerra Híbrida (Tradução do Autor)
Fonte http://www.frontiere.eu/confinamiento-global/esquema-guerra-hibrida

Conforme Visacro (2018), os cenários que dão forma às áreas conflagradas, ao redor do planeta, têm se destacado por sua complexidade, não linearidade, instabilidade, imprevisibilidade, heterogeneidade, mutabilidade e dinamismo.

As principais características do campo de batalha do século XXI são: níveis variáveis de intensidade de conflito; ameaças provenientes de atores estatais e não estatais; população civil, com postura ambivalente; idiossincrasias culturais (complexidade do “terreno humano”); onipresença da mídia; assédio de organismos de defesa dos direitos humanos; outras agências estatais presentes, no interior da área de operações; atuação de organizações não governamentais; restrições legais; limites impostos pela opinião pública; controle de danos, sobre bens civis e o meio ambiente; disponibilidade de moderna tecnologia; grande volume de dados; velocidade e fluidez da informação; e disseminação da informação, em escala global.

Descortinam-se ameaças concretas, que exigem dos Estados a geração de capacidades, para o combate ao terrorismo; para a proteção da sociedade, contra as armas de destruição em massa; a participação em missões de manutenção e/ou imposição da paz, sob a égide de organismos internacionais; e o controle de contingentes populacionais ou de recursos escassos (energia, água ou alimentos) (BRASIL, 2013).

A PND e a END descrevem o atual cenário, no qual estamos inseridos e apresentam as suas diretrizes para as Forças Armadas.

Nesse contexto, o Exército Brasileiro aprovou as Bases de Transformação da Doutrina Militar Terrestre, por intermédio da Portaria nº 197-EME, de 26 de setembro de 2013, destinada a orientar a introdução de concepções e conceitos doutrinários, com vistas à incorporação, na Força Terrestre, das capacidades e das competências necessárias ao seu emprego, na Era do Conhecimento.

As forças devem estar aptas a conduzir Operações, no Amplo Espectro, combinando atitudes, simultânea ou sucessivamente, em operações ofensivas, defensivas, de pacificação e de apoio a órgãos governamentais, tudo isso em um ambiente conjunto e interagências e, por vezes, multinacional (BRASIL, 2013).

3.3 A GUERRA ASSIMÉTRICA

Os avançados meios de TI, aliados a armamentos cada vez mais eficientes dos Estados desenvolvidos (em contraposição à Estados ou facções com baixas capacidades político-econômico-militares), fazem com que esses últimos acabem por adotar o confronto não linear; a insurgência; e o combate de guerrilha, como doutrina, configurando o que hoje é chamado de “guerra assimétrica” (METZ, 2001).

Esse tipo de conflito costuma, ainda, desenvolver-se em áreas urbanas, com larga presença de civis. As suas principais motivações são os objetivos político-econômicos, sendo os efeitos psicológicos do conflito, amplamente, utilizados para atingi-los, gerando uma espécie de conflito híbrido, onde se destaca o emprego de ações de operações psicológicas e de combate irregular (HAMMES, 2007).

3.4 O COMANDO E CONTROLE (C^2)

Os novos conceitos de Guerra dinamizaram os conflitos e exigem que os comandantes, em todos os níveis, consigam exercer a direção das ações, desenvolvendo a consciência situacional sobre todo o espectro do Campo de Batalha. O sistema de C^2 tem sido desenvolvido para permitir o gerenciamento das Operações.

O avanço das TI; o incremento das relações econômicas, financeiras e comerciais; e o crescente enfoque multilateral em questões socioambientais, têm gerado situações de crise entre os Estados. É imperioso que os decisores político-militares sejam capazes de acelerar o seu ciclo de tomada de decisão, maximizando oportunidades e minimizando fraquezas do poder nacional.

O Ministério da Defesa (MD) tem investido no desenvolvimento continuado do SIPLOM, que consiste no seu componente de *software* de C^2. Ele integra o SISMC2

sendo empregado para a obtenção de uma Consciência Situacional do Teatro de Operações, auxiliando os decisores nos seus processos de tomada de decisão.

Segundo o Manual MD31-M-03/2015, “o conceito de C² envolve três componentes imprescindíveis e interdependentes:

- A **Autoridade** – desenvolvimento e exercício da liderança, em todos os níveis, a fim de que as suas decisões conduzam aos objetivos desejados;

- O **Processo Decisório** – que consiste na metodologia e na execução do planejamento para a tomada de decisão e acompanhamento; e

- A **Infraestrutura** – traduzida por componentes indispensáveis para o exercício do C², empregando meios, tecnologias e técnicas especializadas.

Nesse trabalho, procurar-se-á realizar um debate acerca desse terceiro componente, onde estão inseridas a Arma de Comunicações e as suas novas tecnologias, além da presença do que se sinaliza como as novas “Vertentes” do C², a Guerra Eletrônica e a Guerra Cibernética.

O Sistema de C² é o conjunto de instalações, equipamentos, sistemas de informação, comunicações, doutrinas, procedimentos e pessoal essenciais para o decisor planejar, dirigir e controlar as ações da sua organização (Brasil, 2015).

A estrutura do Sistema de C² é formada pelas Tecnologias de Informação e Comunicações (TIC), recursos e ferramentas, por meio das quais as informações são coletadas, monitoradas, armazenadas, processadas, fundidas e disseminadas, além de centros de C² e postos de comando.

NÓBREGA (2019) apresenta a Política de C², no nível MD, abordando as características e servidões, das novas concepções do C²:

- As informações e as ordens devem fluir mais próximo possível do tempo real;

- A massa de informações disponíveis para a tomada de decisão é enorme e de toda ordem, tornando o processo decisório exaustivo e complexo;

- As decisões devem ser tomadas, em prazos cada vez mais abreviados; e

- As informações das ações chegam a quem deve decidir e podem alcançar toda sociedade, devido à ação da mídia (competente e ávida por notícias); as decisões, podem sofrer influência quase instantaneamente da opinião pública.

Os SISMC² são concebidos para atender às demandas das Forças Armadas, que possuem seus sistemas próprios, com doutrina e equipamentos distintos, em razão das especificidades operativas e das peculiaridades de equipamento e doutrina.

Na literatura norte-americana, a sigla C² evoluiu para C³I (Comando, Controle e Inteligência), na década de 1990; depois, incorporou mais um “c”, tornando-se C4I, com a inclusão dos computadores nos sistemas; e, finalmente, o termo C4ISTAR, acrescentando os termos vigilância, aquisição de alvos e reconhecimento”.

O Catálogo de Capacidades do EB (Manual EB20-C-07.001), elaborado pelo EME, estabelece que o Sistema de C² deve ser capaz de:

> “proporcionar, ao Cmt, em todos os níveis de decisão, o exercício do C², por meio da avaliação da situação e da tomada de decisões, baseada em um processo eficaz de planejamento, de preparação, de execução e de avaliação das operações”

A infraestrutura de Comunicações é baseada na distribuição de Centros de Comunicações, no campo de batalha, estabelecendo ligações entre os escalões superiores e subordinados, constituídos por: centros de operações, centros de dados, sistemas de informação, em apoio ao planejamento e à visualização das operações e demais atividades de interesse; recursos de TIC; e salas de reunião (BRASIL, 2015).

As novas tecnologias permitiram comunicações eficazes a longas distâncias, ampliando o campo de batalha, em todas as dimensões.

A facilidade de acompanhar as operações à distância reforça a tendência ao micro gerenciamento - interferência excessiva dos escalões superiores, nas decisões das pequenas frações - criando o dilema a respeito de quem está em melhores condições de tomar as decisões: escalões inferiores aferrados no terreno; ou comandantes, que acompanham a crise à distância (Visacro, 2015).

O Manual EB20-MF-10.102 (DMT, 2014) definiu no EB as funções de combate e estabeleceu que a função C² é a responsável pela integração das demais funções: movimento e manobra, inteligência, fogos, logística e proteção.

O Manual de Campanha EB20-MC-10.205 estabeleceu as bases doutrinárias para o C², alinhadas às concepções definidas pelo MD, ressaltando os componentes do Sistema de C², que são os equipamentos, o pessoal e os procedimentos. Quanto mais rápido ocorrer o ciclo OODA (observar, orientar, decidir e agir) mais ágil é o processo decisório.

3.5 “CYBERWAR”, NO CONTEXTO DO CONFLITO DE QUINTA GERAÇÃO

Acrescente-se ao descrito sobre conflitos de quarta geração (Guerra Híbrida) e guerra assimétrica, o incremento tecnológico em constante desenvolvimento, no

século XXI, e teremos aquilo que estudiosos dos fenômenos de guerra e paz denominam de “guerra de quinta geração (5GW)”.

A próxima geração de guerras estará atrelada às recentes evoluções tecnológicas, se estendendo ao meio cibernético - a “*cyberwar”* (HAMMES, 2007).

O emprego de ataques cibernéticos é bem lógico; um ataque cibernético coordenado, sobre infraestruturas críticas, como energia e telecomunicações pode causar maior dano do que um arrebatamento por um bombardeio convencional.

Existem questões a serem respondidas: um indivíduo sentado em frente ao computador, de seu apartamento, invadindo o sistema de segurança de uma usina nuclear, pode ser considerado um combatente, à luz do direito internacional dos conflitos armados? Um contra-ataque seria justificável?

Essas questões inexistiam durante as Convenções de Genebra e devem permear os debates acerca dos conflitos de quinta geração pelos próximos anos, tanto nas academias, quanto nos centros de estratégia e doutrina militares.

É importante entender o conceito de território cibernético - trata-se de um espaço, onde não há fronteiras físicas e no qual diferentes atores “navegam”, livremente, com exceção para os domínios protegidos por um ente, público ou privado, que exerça seus direitos sobre ele. É composto por duas partes: uma estrutura não física - dados e informações - e uma estrutura física - equipamentos, *data center* e servidores. (PINHEIRO, 2013).

A “*cyberwar”* pode ocorrer, na medida em que, a “política por outros meios”, definição de Clausewitz, é feita por ataque aos domínios do espaço cibernético, onde predomina certa soberania, por parte de quem o detém (NYE, 2001).

Os grupos organizados de ativistas *hackers*, organizações criminosas e agências estatais e não estatais, contemplam boa parte dos que podem agir, nesse campo específico.

4 DESENVOLVIMENTO

A seguir, serão apresentados conceitos e a importância do desenvolvimento de novas tecnologias de comunicações, empregados nos conflitos atuais.

Destaque-se a exploração do espectro eletromagnético e do ciberespaço pela Guerra Eletrônica e a Guerra Cibernética, respectivamente, indicando a necessidade de mudar a mentalidade de exploração e utilização das Comunicações.

No combate moderno, o emprego das Forças militares, tem sido influenciado pelo rápido avanço tecnológico, decisivo para a precisão das manobras; para a letalidade dos sistemas de armas; para deslocamentos acelerados de forças militares; para aumento dos limites de atuação; para um maior sincronismo das ações táticas e um mais amplo conhecimento sobre a força oponente.

Essa evolução criou novas possibilidades e vulnerabilidades, pois as emissões indiscriminadas de sinais eletromagnéticos e de informações, no ciberespaço oferecem, ao oponente, a possibilidade de explorá-lo, em seu próprio proveito.

4.1 GUERRA ELETRÔNICA

4.1.1 Definições

O Manual C34-1, do EB define a GE como sendo um conjunto de ações, que devem ser desencadeadas, com a finalidade de assegurar o emprego eficiente e seguro das comunicações orgânicas e, ao mesmo tempo, devem procurar impedir, dificultar ou tirar proveito das emissões inimigas.

A GE no nível tático, desenvolve-se junto às operações militares e se refere à situação imediata do campo de batalha, atuando sobre as comunicações, sistemas de armas, de vigilância e sobre outros sistemas eletrônicos amigos, ou não.

Nos níveis mais elevados, avulta a importância do trabalho da Inteligência do Sinal (Intlg), deve-se buscar dados sobre os equipamentos de Comunicações e Não Comunicações dos potenciais adversários, monitorando redes civis e militares, com o propósito de formar conhecimento sobre sinais de interesse do inimigo.

A GE introduziu uma nova dimensão do combate, tão importante quanto a manobra, o fogo e o movimento: “o domínio do espectro eletromagnético”.

O Manual C34-1 apresenta a definição da missão geral da GE: “apoiar as forças em operações proporcionando, a partir dos sinais eletromagnéticos interceptados: conhecimento sobre o oponente; proteção aos sistemas eletrônicos amigos; e óbices aos sistemas do oponente, de forma a restringir ou impedir a sua eficiência.

4.1.2 Histórico da GE e momentos marcantes

Os historiadores e estudiosos sobre o assunto consideram, como marco inicial da GE, a Batalha Naval de *Tsushima*, ocorrida na Guerra Russo-Japonesa, em 1905, onde ocorreu uma interceptação pela esquadra russa, sobre as comunicações de telegrafia sem fio do cruzador auxiliar *Shimano Maru, decidindo a* Guerra.

No período entre as duas grandes guerras mundiais, a aplicação da tecnologia nos domínios das comunicações permitiu o desenvolvimento de métodos e processos de criptografia, buscando-se aumentar a segurança nas comunicações.

Em 1938, antecedendo a II GM, a Grã Bretanha instalou, na Costa Sul das Ilhas Britânicas, uma rede de radares, com a finalidade de controlar o Canal da Mancha, considerando-se a hipótese de um conflito com a Alemanha.

Em 1939, foi registrada a primeira missão de Inteligência do Sinal no campo das Não Comunicações, realizada com o emprego do dirigível *Graf Zeppelin* (do exército Alemão), objetivando rastrear a rede de radares britânicos.

Em 1940, na Batalha da Grã-Bretanha, foram desenvolvidas ações de GE, contra os sistemas de navegação e bombardeio utilizados pela Força Aérea Alemã. Por outro lado, a Alemanha instalou uma verdadeira muralha radar para detectar a penetração dos aviões britânicos e Norte Americanos, sobre o solo alemão.

A Guerra do Vietnã apresentou novos aspectos operacionais: o surgimento de missões *"Wild Weasel",* organizadas pelos americanos, para neutralizar e/ou destruir os sistemas de armas antiaéreos dirigidos por radares; e dispositivos de salto e agilização de frequência para conjuntos-rádio e radares.

Os conflitos entre Israel e os países árabes (Guerra dos Seis Dias e *Yom Kippur*) apresentaram novas características para a GE, pela apresentação de dispositivos de elevada tecnologia, tais como o "radar-*doppler*"; os mísseis infravermelhos portáteis; os mísseis anticarro comandados por fio; o emprego de engodos infravermelhos; e os veículos aéreos não tripulados (VANT) e eletro-ópticos.

O conflito no Atlântico Sul entre a Argentina e Grã-Bretanha (Guerra das Malvinas), em 1982, marcou a entrada definitiva da GE, como fator para multiplicar o poder de combate. A Grã-Bretanha fez amplo emprego de bloqueadores eletrônicos, para dificultar as comunicações e o exercício do C^2, entre as tropas argentinas desdobradas nas ilhas Malvinas e o comando das Forças Armadas em Buenos Aires.

Na Guerra do Golfo o Iraque ficou imobilizado, sendo incapaz de infringir danos às forças aliadas. Sensores e atuadores, operando no espectro eletromagnético, interferiram nas comunicações, neutralizando sistemas de defesa e garantindo uma supremacia eletromagnética, anulando pontos vitais de defesa e do sistema logístico. O Iraque foi reduzido a um contendor cego, surdo, mudo, imobilizado e desprovido de vontade de lutar, causando uma rendição incondicional iraquiana (AMARANTE, 2003).

No século XXI, a Guerra da Síria comprovou a importância da supremacia eletromagnética. A Síria se tornou um ambiente eletromagnético extremamente agressivo, dificultando o emprego dos sistemas de posicionamento - *Global Positioning System* (GPS), os enlaces de comunicações e o uso de radares.

4.1.3 Depoimentos Históricos

Alguns depoimentos históricos ilustram a importância da GE:

- "... a próxima Guerra será vencida pelo lado que melhor explorar o espectro eletromagnético..." (Almirante *Sergei Gorshkov* – marinha russa, 1987);

- "... os Estados Unidos entendem que, realizando interferência sobre um radar inimigo, somente será eliminada uma única arma. Entretanto, interferindo nos seus sistemas de C3, um completo arsenal pode ser destruído..." (Sr. William J. Perry, ex-subsecretário de defesa dos EUA);

- "... Na Guerra do Golfo, o sistema de C^2 das Forças de Coalizão se mostrou pouco vulnerável à ação do inimigo iraquiano, em especial porque o sistema de Comunicações, que lhe deu suporte, priorizou as informações em dados digitais, minimizando as comunicações por voz e pelos recursos de GE, que possuíam em seus equipamentos..." (COTer, 2020).

- "... As Comunicações englobam os meios básicos para assegurar o controle da tropa. A perda das comunicações é a perda do controle da tropa; e a perda do controle da tropa na batalha, invariavelmente, conduz à derrota" (*TITOV*, 1979).

- O Cel José Corrêa Oliveira foi o principal responsável pela entrada do Brasil, no seleto grupo de países com GE. Ele descrevia a mesma como sendo "uma guerra silenciosa, invisível e a mais secreta das guerras".

A GE é uma consequência direta da evolução da tecnologia de detecção e comunicações, ocorrida durante e depois da II GM. A invenção dos radares; e o aperfeiçoamento dos sistemas de interceptação e de interferência de ondas de rádio e da criptografia revolucionaram a forma como se fazia a guerra, até então.

4.1.4 A Guerra Eletrônica brasileira: infraestrutura, doutrina e incidências.

A fim de aumentar a capacidade operacional do Exército, nas áreas de Comunicações e GE, foi ativado, em 20 de fevereiro de 2009, o Comando de Comunicações e GE do EB – CCOMGEX - que tem por missão atuar em proveito da Força Terrestre, aumentando a operacionalidade, pelo desempenho de atividades nas

vertentes Operacional, de Ensino e de Logística, bem como gerenciando a Inteligência do Sinal e cooperando, na área de Ciência e Tecnologia.

Durante a década de 1970 e início de 1980, o Cel Humberto José Corrêa de Oliveira tentava chamar a atenção para esse tema, em artigos publicados, na Revista Militar Brasileira. Em “Reflexões sobre Guerra Eletrônica”, publicado em 1980, pode-se destacar um trecho onde Napoleão I disse que “Os Exércitos marcham sobre os seus estômagos”. No presente, é mais correto dizer: “Os Exércitos marcham sobre a sua eletrônica, pois não há aspecto da guerra moderna, do qual ela não participe.”

Atualmente, o CCOMGEX mantém agrupado, em seu aquartelamento: os procedimentos de logística da classe VII (Material de Comunicações); o Ensino e o emprego de Comunicações e Guerra Eletrônica e as atividades de coordenação e planejamento do Projeto do Sistema Integrado de Monitoramento de Fronteira (SISFRON).

4.2 GUERRA CIBERNÉTICA

4.2.1 Definições

É a não autorizada penetração: por, ou em nome de, ou em apoio a um governo, em computador ou rede de outra nação; ou qualquer outra atividade, afetando um sistema computacional, com o propósito é incluir, alterar ou falsificar dado; ou causar a interrupção; ou danos a um computador; ou a dispositivos de rede; ou a objetos, que dado computador controla (*CLARKE*; *KNAKE*, 2010).

Essa vertente das Comunicações tem potencial de interromper o ciclo de C2, mediante ações sobre os recursos de TI da infraestrutura dos centros de C2 e respectivas redes e terminais. Além disso, recentes sistemas controlados por computadores têm sido avariados pela ação de vírus injetados, maliciosamente.

Tais vírus modificam os programas controladores, denominados códigos-fonte, das máquinas que estão sendo atacadas, de modo que obedeçam a instruções intrusas, capazes de provocar efeitos perniciosos. Centrais de energia, armamentos e propulsores são alguns exemplos de sistemas de meios táticos, que podem ser danificados por vírus, como o *“Stuxnet”, que será visto posteriormente.*

No século XXI, o fenômeno das “*Fake News*”, ou notícias falsas, surgiu como mais uma ameaça ao C², podendo ser usada em campanhas de desinformação, para denegrir o oponente, conquistar apoio da opinião pública e vencer os conflitos, sendo uma arma contra os aspectos cognitivos dos decisores e da rede de apoio. A

população brasileira se destaca como uma das mais preocupadas do mundo com o fenômeno das “Fake News”.

Figura 3. Brasil é o país onde há mais preocupação com *Fake News*

Fonte: www.poder360.com.br. Acesso: 12 Ago 22.

4.2.2 Histórico do emprego da Guerra Cibernética e reflexões importantes

Por Ataque Cibernético tomaremos a seguinte definição contida na proposta de Política Nacional de Inteligência para o Brasil, elaborada pelo GSI/PR, em 2009:

> […] referem-se a ações deliberadas, com o emprego de recursos da Tecnologia da Informação e Comunicações (TIC), que visem interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados essenciais à sociedade e ao Estado, a exemplo daqueles pertencentes à infraestrutura crítica nacional. Os prejuízos decorrem, também, da manipulação de opiniões, mediante ações de propaganda ou de desinformação […].

O início da Guerra Cibernética é controverso, mas, provavelmente, o primeiro caso teria ocorrido em 1982, com a explosão do gasoduto Transiberiano, que teria sido causada pela introdução, pelo serviço secreto dos EUA, de um *“bug”,* no software do sistema de gerenciamento e prospecção de gás, roubado pela KGB de uma empresa canadense. Segundo *REED* (2005), foi a mais monumental explosão não nuclear vista do espaço.

Em 2007, a Estônia foi alvo de uma série de ataques cibernéticos, que afetaram, de forma significativa, serviços essenciais do país. Tais ataques foram causados por uma luta política entre os estonianos e os líderes soviéticos, pela remoção de estátuas, que lembravam o domínio do país pelos russos.

A Estônia foi atingida por um ataque DDoS de grande escala, lançado por diversas "*botnets",* que durou semanas e derrubou serviços eletrônicos do governo, bancos, sites de jornais e servidores da rede de telefonia.

Outro ataque cibernético conhecido ocorreu em 2008, na Geórgia (*SHAKARIAN,* 2011), durante a chamada Guerra Russo-Georgiana. Na época, a Ossétia do Sul era reconhecida, internacionalmente, como território da Geórgia. No entanto, se considerava independente, recebia proteção, financiamento e vivia sob influência russa (*CLARK; KNAKE*, 2010).

Naquele ano, rebeldes da Ossétia do Sul organizaram uma série de ataques com mísseis, contra aldeias da Geórgia. Em resposta, a Geórgia bombardeou a capital da Ossétia do Sul e invadiu a região. No dia seguinte à invasão georgiana, veio a resposta do exército russo, expulsando os militares georgianos da Ossétia do Sul.

Ocorre que a ofensiva física não foi a única deflagrada contra a Geórgia. Ao longo do conflito, a Geórgia sofreu ataques "DDoS" direcionados aos seus meios de comunicação, os sistemas bancários, de cartões de crédito e de telefonia móvel foram afetados. A maioria dos roteadores que conectavam a Geórgia à Internet, via Turquia e Rússia, foram atacados. A Geórgia perdeu o acesso às fontes de informação e notícia externas.

Um novo tipo de ataque veio à discussão com a Operação *Orchard*, lançada em 2007 pelo Estado de Israel, contra a Síria. Na madrugada de 06 de setembro de 2007, aeronaves da Força Aérea Israelense entraram no espaço aéreo sírio e bombardearam uma instalação industrial, que estava sendo construída no território daquele país. Tal instalação era uma planta nuclear, que a Síria estava construindo, com o apoio da Coréia do Norte.

Os militares sírios observavam, atentamente, seus radares, mas no momento em que as aeronaves F-15 *Eagles* e F-16 *Falcons* de Israel invadiram o espaço aéreo sírio, nada de incomum apareceu nas telas dos radares do sistema de vigilância. Analistas sugeriram que o país tenha sido vítima de um ataque de guerra eletrônica. No entanto, o ataque se diferenciava das demais Medidas de Ataque Eletrônico conhecidas, por explorar uma vulnerabilidade implantada no domínio cibernético do sistema de vigilância sírio (*ADEE*, 2008; *CLARK; KNAKE*, 2010).

Em 2010, um ataque usando o "*malware Stuxnet*" foi lançado contra o sistema "SCADA", responsável pelo controle de centrífugas de enriquecimento de Urânio, na

usina de *Natanz*, com o objetivo de negação de armas nucleares ao Irã, de forma furtiva e sem o emprego de armas físicas.

Uma vez encontrando o sistema alvo – CPLs *Siemens* conectados às centrífugas, o *worm* liberava "ogivas digitais", que se instalavam nos CLPs e iniciavam ações sutis de degradação e destruição das centrífugas.

No mais atual caso de uso da *"cyberwar"*, em cenários de conflitos assimétricos, os EUA realizaram ataques contra a organização terrorista Estado Islâmico, em território sírio. Os ataques visaram impedir coordenações táticas, por parte das lideranças do grupo terrorista, ao fazerem uso de equipamentos TI.

As ações de guerra cibernética apresentadas não esgotam os ataques cibernéticos já ocorridos. No entanto, demonstram a diversidade de possibilidades de uso dessas ferramentas, para causar danos a nações adversárias ou mesmo para apoiar a execução de ataques cinéticos, em operações militares.

CLARKE e *KNAKE* (2010) defendem que a capacidade de um país, num conflito desse tipo, é medida em três dimensões: **ofensiva** - atacar outros atores estatais; **defensiva** - bloquear e/ou reduzir o estrago derivado do ataque e **dependência** – a vulnerabilidade do sistema de computadores de um país.

No entender de diversos escritores, os EUA têm a maior capacidade ofensiva, mas a China e a Coréia do Norte possuem maior capacidade de defesa, pois podem desligar sua internet e se isolarem do mundo.

Mesmo que a possibilidade de mortes, em ataque cibernético, seja baixa, um ataque a sistemas de computadores pode ser maciçamente disruptivo, deixando um país impotente diante da ação de um adversário (tanto militar, como econômico). A internet pode ser utilizada, ainda, para o roubo de segredos industriais e militares.

A rede mundial de computadores poderá viabilizar a ideia de Sun Tzu, da guerra ser vencida sem o inimigo estar em conflito, pela completa incapacidade de um ator utilizar a sua capacidade econômica e a força militar, contra o seu adversário.

4.2.3 A defesa cibernética brasileira: infraestrutura, doutrina e incidências.

O tema ganhou agenda nacional, em 2008, ao ser previsto na Estratégia Nacional de Defesa (END), como um dos setores estratégicos, ao lado do aeroespacial e do nuclear (BRASIL, 2008, p.6), ficando a defesa cibernética a cargo do Exército Brasileiro.

Em sua redação, a END destaca, que devem ser adotadas medidas para a segurança das áreas de infraestrutura críticas e, ainda, prevê:

> "As capacitações cibernéticas destinar-se-ão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação, entre todos os contingentes das Forças Armadas, de modo a assegurar a sua capacidade para atuar em rede".

No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética, nos campos industrial e militar.

> (...) Dar-se-á o aperfeiçoamento dos dispositivos e dos procedimentos de segurança, que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos; e, se for o caso, que permitam o seu pronto restabelecimento, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, das Comunicações, da Ciência e Tecnologia, e do GSI-PR." (Brasil, 2008,)

A END fomenta que as Forças Armadas tenham, como objetivo, a melhoria da capacidade de Comando, Controle, Comunicações, Computação e Inteligência (C4) utilizando, como meio, as ferramentas de TIC.

Existe uma distinção entre os conceitos de Segurança e de Defesa Cibernética:

- A Segurança Cibernética consiste na proteção das redes de comunicação, com cooperação entre os órgãos públicos e privados, para a garantia do funcionamento das infraestruturas críticas civis brasileiras.

- A Defesa Cibernética tem uma maior relação com a defesa e pronta resposta ativa, em casos de crise, funcionando também como um módulo em permanente vigília, em condições de neutralizar ameaças.

A Segurança Cibernética foi atribuída, no Brasil, ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), enquanto a Defesa Cibernética ficou a cargo das Forças Armadas.

No contexto do MD, as ações no espaço cibernético dividem-se em:

- **Nível político** - Segurança da Informação e Comunicações (SIC) e Segurança Cibernética - coordenadas pela Presidência da República;

- **Nível estratégico** - Defesa Cibernética - a cargo do MD, Estado-Maior Conjunto das Forças Armadas (EMCFA) e comandos das FA; e

- **Níveis operacional e tático** - Guerra Cibernética - restrita, ao âmbito interno das FA.

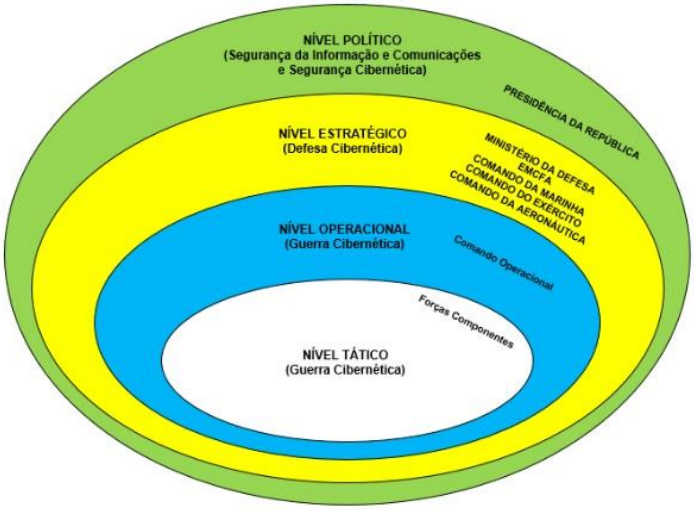

Figura 4 – Níveis de decisão
Fonte Manual de Guerra Cibernética EB70-MC-10.232

O Exército criou o Centro de Defesa Cibernética (CDCiber), em 2010, visando integrar as forças de defesa, na proteção do ambiente cibernético, no que diz respeito às infraestruturas próprias à defesa e à soberania nacionais, ou seja, também atua no campo da Segurança Cibernética, protegendo infraestruturas críticas nacionais.

Para o adestramento em "*cyberwar"*, o CDCiber conta com equipamento simulador de conflitos digitais, que possibilita exercitar os procedimentos operacionais, para os diversos tipos de ataques virtuais simulados possíveis; atualmente, o Brasil sofre cerca de 30 mil ataques diários.

A relevância do assunto pode ser vista na recente Pesquisa Global de Segurança da Informação, realizada pela empresa PWC7, quando se constatou que o número de ataques cibernéticos, no Brasil, incluído fraudes virtuais, subiu 274%, no ano de 2015, enquanto a média de crescimento global foi de 38%.

De acordo com a *Akamai Technologies* (empresa especializada em segurança digital), o Brasil é apontado como o 3° maior propagador de ataques cibernéticos do mundo, com 11% dos casos, ficando atrás apenas de EUA e Rússia.

Figura 5 – Gráfico de 20 países mais afetados por *Crimes Cibernéticos (tradução do Autor)*
(Fonte: http:// https://www.enigmasoftware.com/pt/20-paises-maior-indice-crimes-ciberneticos/)

A empresa *Kaspersky Lab*, no documento denominado *"Beaches, carnivals and cybercrime:* a look inside the Brazilian underground", classifica o país como um dos mais perigosos do mundo, no quesito "*cybercrime",* tendo a maioria dos casos referentes a fraude contra indivíduos e empresas.

4.2.4 Possibilidades e Limitações da Guerra Cibernética, segundo o Manual EB70-MC-10.232

4.2.4.1 São possibilidades da guerra cibernética:

a) atuar no espaço cibernético (ações ofensivas, defensivas e exploratórias);

b) cooperar na produção do conhecimento de inteligência, por meio dos dados obtidos da fonte cibernética;

c) atingir sistemas de informação de um oponente, sem limitação de alcance físico e exposição de tropa;

d) cooperar com a segurança cibernética, inclusive de órgãos externos ao MD, mediante solicitação ou no contexto de uma operação;

e) cooperar com o esforço de mobilização, para assegurar a capacidade dissuasória da guerra cibernética;

f) facilitar a obtenção da surpresa, com base na exploração das vulnerabilidades dos sistemas de informação do oponente;

g) realizar ações contra oponentes com poder de combate superior; e

h) realizar ações com custos significativamente menores, do que aqueles envolvidos nas operações militares, nos demais domínios.

4.2.4.2 Limitações da guerra cibernética:

a) restrita capacidade de identificação da origem e de atribuição de responsabilidades por ataques cibernéticos;

b) restrita eficácia das ações cibernéticas defensivas, devido à existência de vulnerabilidades nos sistemas computacionais;

c) restrita capacidade de gestão de pessoas, particularmente, no que concerne à identificação, à seleção, à capacitação e à retenção de talentos;

d) dificuldade de acompanhamento da evolução tecnológica, na área cibernética; e

e) possibilidade de ser surpreendido, com base nas vulnerabilidades dos próprios sistemas de informação.

4.2.5 Capacidades Operativas da Guerra Cibernética, segundo o Manual 3-4 EB70-MC-10.232.

A cibernética possui 3(três) capacidades operativas:

- **Proteção Cibernética** – ações para neutralizar ataques e exploração cibernética contra dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações em uma situação de crise ou conflito;

- **Ataque Cibernético** - ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados, em dispositivos e redes de computadores e de comunicações do oponente;

- **Exploração Cibernética** - ações de busca ou coleta nos Sistemas de TI de interesse, a fim de obter dados. Evitar que essas ações sejam rastreadas e sirvam para a produzir conhecimento ou identificar as vulnerabilidades desses sistemas.

4.3 A CONVERGÊNCIA DA GUERRA ELETRÔNICA E DA GUERRA CIBERNÉTICA AO C², SEGUNDO NETO (2018)

O Manual EB-20-MC10.213, Operações de Informação, faz a seguinte menção à integração de Ações Cibernéticas e de GE:

> Normalmente, as ações cibernéticas e eletromagnéticas são atividades desenvolvidas para apreender, reter e explorar uma vantagem sobre oponentes ou potenciais adversários, tanto no espaço cibernético como no espectro eletromagnético; e, simultaneamente, negar e degradar, ao adversário, a utilização dessa vantagem, bem como proteger o nosso processo decisório, particularmente o sistema de comando e controle (BRASIL, 2014).

Nesse mesmo Manual, é dito que a integração da G Ciber com a GE permite que elementos da F Ter garantam e mantenham a liberdade de ação, no espaço cibernético e eletromagnético para as nossas forças, enquanto buscam explorá-la e negá-la aos oponentes.

Tais vetores se apoiam mutuamente e a integração das referidas capacidades são um facilitador, uma vez que contribuem para afetar a percepção e a tomada de decisão do adversário.

Portanto, quando desencadeadas para influenciar um resultado cognitivo, as atividades cibernéticas e os componentes eletromagnéticos são considerados capacidades relacionadas à informação, que devem ser sincronizadas e integradas pelas Operações de Informação.

No conceito operativo do Exército, em amplo espectro, as ações ofensivas de G Ciber, no nível tático, são conduzidas no âmbito das unidades de GE, por meio das frações respectivas, sobretudo em razão da convergência conceitual e funcional, além de certa similaridade entre os alvos atuais atinentes às duas atividades.

As funções operativas de G Ciber são conduzidas pelo emprego de “*malwares* e *spywares*”; e as funções de GE, são desencadeadas por meio de radiação, retransmissão, exploração, execução de procedimentos e adoção de tecnologias associadas ao espectro eletromagnético.

A maior parte dos sistemas táticos atuais, sejam de telecomunicações ou de sensoriamento, são integrados logicamente, formando extensas redes com considerável capacidade computacional e mobilidade; essa última característica é decorrente dos enlaces baseados na emissão de sinais eletromagnéticos.

Nesses casos, o espectro eletromagnético é o principal ponto comum entre as atividades de GE e G Ciber.

Existe a necessidade de planejamento conjunto e sincrônico das ações de GE e G Ciber, sob pena de eventual interferência, por exemplo, das ações de GE sobre

as atividades desenvolvidas pela G Ciber em redes, onde o espectro eletromagnético é o canal, no qual elas têm suporte.

O Exército Norte Americano, em 2014, define as Atividades Ciber Eletromagnéticas - em inglês, "*Cyber Electromagnetic Activities* (CEMA)", como a direção para que as forças terrestres operem o ciberespaço e o eletromagnético. As ações militares, no mundo, são fortemente dependentes de redes; assim, a unificação dessas duas formas de guerra tem o objetivo de permitir, aos EUA, a vantagem sobre os inimigos, degradando e/ou negando o uso desse espaço (Figura

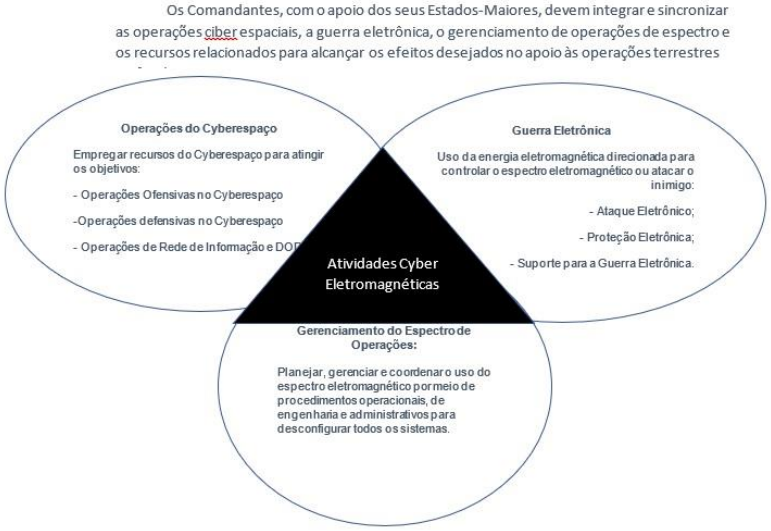

Figura 6 - Atividades Ciber Eletromagnéticas (Tradução do Autor)
Fonte: United *States Army* 2014.

O ciberespaço e as emissões eletromagnéticas, hoje, são os principais meios de transmitir conhecimento e informações, sejam elas militares ou não. Pode-se afirmar que as redes de computadores e de comunicações, no século XXI, são convergentes, pois existe íntima interligação entre computadores, equipamentos de comunicações e eletrônicos, "softwares" e criptografia.

A convergência entre as armas cibernéticas e o aspecto eletromagnético está centrada em um conceito fundamental: **a guerra centrada em redes**, ou seja, uma abordagem de guerra, que utiliza toda a tecnologia eletromagnética e de rede, para conseguir a maior consciência situacional possível, no campo de batalha, buscando: acompanhar a evolução do conflito; a sincronização das ações; e impedir que o adversário tenha acesso ao seu arsenal de GE e G Ciber.

Conceitos antes vistos como ambientes completamente diferentes têm sido percebidos, cada vez mais, como partes de uma mesma forma de conceber a guerra.

5 ANÁLISE DO TRABALHO E/OU EVIDÊNCIAS

Ao encerrar o estudo bibliográfico e documental sobre o assunto deste trabalho fica evidente, por meio da análise do conteúdo apresentado, que as comunicações de hoje não podem ser comparadas com as realizadas no passado.

As novas tecnologias e as novas vertentes da Arma do Comando: a Guerra Eletrônica; e a Guerra Cibernética mudaram a exploração do espectro eletromagnético e criaram um novo espectro de atividades, conhecido como “Atividades Ciber Eletromagnéticas”.

É possível, também, observar que as autoridades brasileiras já entenderam a necessidade de se aprofundar nesses novos aspectos dos conflitos modernos, com a criação do CCOMGEx e do Centro de Defesa Cibernética, respectivamente, para atuar sobre a Guerra Eletrônica e a Guerra Cibernética.

Nesse mesmo diapasão, foram criados o Centro de Instrução de Guerra Eletrônica e a Escola de Defesa Cibernética, para formar especialistas em GE e GCiber.

A análise do trabalho apresentado também mostra que, a cada dia, novas tecnologias são criadas e o constante aperfeiçoamento é necessário, para fazer frente aos novos perigos desenvolvidos como “*softwares* e *malwares*” criados para agir sobre as redes, sejam elas físicas ou *wireless*.

Um grande problema para o Brasil é a necessidade de recursos financeiros para investir em treinamento, estrutura física e equipamentos necessários para proteger as redes brasileiras, quanto a ataques eletromagnéticos e/ou cibernéticos.

Os dados apresentados demonstram que o Brasil é um dos países mais afetados em todo o mundo, por ataques dessa natureza, principalmente, sobre as estruturas financeiras.

Da mesma forma, os diversos exemplos de ataques cibernéticos e usos da GE, ao longo da história, evidenciam como as estruturas podem ser afetadas e as implicações causadas por ataques planejados e direcionados, além da sensibilidade de acesso as informações, que podem sofrer espionagem, a todo o momento.

6 MELHORES PRÁTICAS

Tendo em vista as informações apresentadas neste trabalho e a experiência do autor, com mais de 30 anos de serviços prestados ao EB; como integrante da Arma de Comunicações, participando de inúmeros exercícios e operações militares, em território nacional e em missão de paz - Missão das Nações Unidas para Estabilização do Haiti (MINUSTAH); é possível elencar algumas práticas, que podem contribuir com a mudança de mentalidade sobre a Arma de Comunicações:

- Investir na montagem de infraestrutura adequada, para proteção de instalações e redes, além de permitir melhores condições de treinamento e aprimoramento do pessoal;

- Montar informativos e notas técnicas, que detalhem os principais acontecimentos de atividades *cyber* eletromagnéticas, buscando apontar falhas cometidas, normas negligenciadas, as melhores práticas e oportunidades de melhoria;

- Realizar exercícios para treinamento de operação dos equipamentos e pessoal, que estejam ligados às atividades *cyber* eletromagnéticas, permitindo a compreensão e o adestramento das técnicas, que devam ser desenvolvidas;

- Permitir a participação do pessoal ligado às atividades *cyber* eletromagnéticas, em fóruns nacionais e internacionais; e cursos no país e no exterior, ligados a esses assuntos, com o intuito de adquirir conhecimentos importantes ao desenvolvimento e aprimoramento dessas atividades;

- Realizar estágios setoriais, em todo o Brasil, com o intuito de difundir conhecimentos e alertar os diferentes segmentos da sociedade, para as necessidades de prevenção e proteção de diferentes instalações. É importante ressaltar que as atividades *cyber* eletromagnéticas impactam não somente instalações militares, devendo ser preocupação de todo país;

- Realizar estágios setoriais destinados ao adestramento das tropas das forças Armadas designadas para desenvolver a mentalidade de emprego das atividades cyber eletromagnéticas, seja para ataque, defesa ou monitoramento e obtenção de informações;

- Desenvolver instruções específicas a serem difundidas, para a prevenção de falhas, na exploração de equipamentos e de dispositivos, diante de atividades *cyber* eletromagnéticas; e que devem ser repassadas para os níveis mais baixos de

operação dos sistemas, a fim de evitar as “brechas”, passíveis de serem utilizadas para invadir e atacar os sistemas.

Não adianta ter normas de utilização, de conhecimento dos usuários do sistema; é necessário treinar os operadores e provedores de acesso;

- Validar a doutrina estabelecida e testar os planejamentos, em caso de ações *cyber* eletromagnéticas perpetradas por uma força adversa;

- Levantar conhecimentos de Interesse, para o aprimoramento da Doutrina existente, por meio de relatórios gerados em Operações e atividades afins;

- As Forças Armadas precisam repensar a necessidade de existir um maior número de especialistas, em atividades cyber eletromagnéticas, a serem desdobrados em diferentes níveis dentro das forças.

É recomendável um processo crescente do número de claros, do mais alto nível da administração, até as organizações militares mais isoladas, mas que estejam interligadas às redes internas das forças e que possam ser utilizadas como porta de entrada, para todo o sistema, por ataques maliciosos.

- As Escolas militares devem aprofundar os seus Planos de Disciplina, em assuntos militares; voltá-los para as Comunicações e as atividades eletromagnéticas, mostrando estudos de caso, melhores práticas e técnicas de proteção dos sistemas. Esses assuntos não devem ser restritos a integrantes da Arma de Comunicações.

7 RECOMENDAÇÕES POLÍTICAS

Da análise realizada, considerando a importância do assunto e com o objetivo de aprimorar a proteção de sistemas e infraestrutura nacionais, recomenda-se:

7.1: **Recomendação n° 01**: estudo do Departamento-Geral do Pessoal, devidamente orientado pelo EME e pelo DCT, para a incorporação de recursos humanos (convocação de temporários) idôneos e qualificados e o preenchimento de claros específicos para o exercício de atividades ligadas à área de cibernética.

Esta recomendação possibilitará a aceleração da implementação de práticas, que permitam uma maior proteção de estruturas sensíveis dentro do país, sejam elas militares ou não.

7.2: **Recomendação n° 02**: solicitação de estudos, por parte do EME, com apoio do DGP, para o aumento sistemático de cargos específicos na tropa, destinados ao

desenvolvimento dos trabalhos em assuntos relativos às atividades *cyber* eletromagnéticas.

Atualmente, as Forças Armadas, em particular o EB, são os únicos que estão preocupados em combater essa ameaça e precisam ser dotados de meios, em especial pessoal habilitado, para bem se desincumbirem nessas atividades.

Esta recomendação poderá ser uma alavanca importante, para a montagem da estrutura necessária ao cumprimento exitoso da missão;

7.2: **Recomendação n° 03**: atualização das Instruções Reguladoras das atividades *cyber* eletromagnéticas, criadas pelo DCT, com apresentação de situações recentes de crise, na área de interesse, apresentando as melhores práticas e os ensinamentos colhidos.

Esta recomendação permitirá a atualização constante dos diferentes usuários do sistema, minimizando os riscos de intrusão.

7.3: **Recomendação n° 04**: realização de Exercícios práticos de atividades *cyber* eletromagnéticas, dentro das forças armadas e, em algumas situações, com a participação de instituições civis, com o intuito de expandir conhecimentos e treinar e desenvolver técnicas de combate a ações perpetradas por uma força hostil.

Esta recomendação possibilitará o desenvolvimento da mentalidade de proteção e emprego de técnicas, contra ações de intrusão dos sistemas estabelecidos;

7.5: **Recomendação n° 05**: solicitação, junto ao Governo Federal, do desenvolvimento de ações coordenadas entre Ministérios, notadamente, entre o Ministério da Defesa e o Ministério da Ciência, Tecnologia e Comunicações (MCTIC), buscando o desenvolvimento de sistemas e o aprimoramento de pessoal em mestrados, doutorados e PhD, nas áreas de interesse das atividades *cyber* eletromagnéticas.

O intuito é o de fortalecer as defesas do Brasil. Esta recomendação objetiva o aumento dos esforços, em busca de um objetivo comum: salvaguardar as estruturas sensíveis do país.

7.6: **Recomendação n° 06**: sensibilizar o governo federal, quanto ao envio de pessoal para participar de cursos e feiras internacionais de tecnologia, que estejam alinhados com a preparação adequada de uma defesa sólida, contra as ameaças desenvolvidas, no *cyber* espaço.

Tal demanda deve ser fruto de uma maior conscientização da sociedade, quanto aos perigos dessa nova realidade.

Em que pese o Brasil ser um dos países mais atacados do mundo, ainda não existem iniciativas conjuntas para minimizar os prejuízos causados.

7.7: **Recomendação n° 07**: buscar a mudança de paradigma, quanto ao emprego da Arma de comunicações, do atual "status" de "arma de apoio ao combate", para "fator decisivo para o sucesso das Operações".

Nos dias atuais, fruto de todo o desenvolvimento tecnológico existente e do surgimento das vertentes da Guerra Eletrônica e da Guerra Cibernética, desde os tempos de paz, a Arma do comando atingiu um novo nível, tão importante quanto a manobra, o fogo e o movimento.

Esta recomendação, se aceita pelo Alto Comando do Exército, oportunizará mudanças, em toda a estrutura da Força.

A guerra do futuro é baseada em alta tecnologia e pode ser resolvida por ataques *ciber* eletromagnéticos, antes do primeiro combate real.

7.7: **Recomendação n° 08**: é extremamente importante, que assuntos ligados as atividades *cyber* eletromagnéticas (GE e GCiber) sejam incluídos, de forma explicita, nos planos de disciplina das escolas de formação militar, programas-padrão das Armas, Quadros e Serviços, em todas as Forças Armadas, com o intuito de acelerar a mudança de mentalidade pretendida, sobre a exploração de meios de TIC.

Esta recomendação deve ser estudada, também, no nível Governo Federal, numa discussão ampla da sociedade, almejando a criação de cursos e políticas de inclusão desses assuntos, em bancos escolares civis, dentro de suas peculiaridades.

Os ataques *ciber* eletromagnéticos podem afetar toda a sociedade, ao incidirem sobre pontos e instalações sensíveis.

8 CONCLUSÃO

O Brasil não convive, atualmente, com perspectivas, no cenário internacional, que apontem para situações de beligerância iminentes. Por isso, nem o Governo destina um orçamento adequado às Forças Armadas, nem a Nação Brasileira mobiliza atenção e energia nessa direção, pois estão envoltos com inúmeras outras questões prioritárias, na vida nacional.

Com o surgimento de tecnologias *cyber* eletromagnéticas que, desde os tempos de paz, são empregadas para causar prejuízos financeiros e obter superioridade sobre outros Estados, surge a necessidade de se combater tais práticas e investir em políticas: que busquem aprimorar as defesas do país; e, ao mesmo tempo, alcem o Brasil, ao seleto grupo daqueles que dominam tais tecnologias.

Na estrutura organizacional do Exército cabe, aos integrantes da Arma de Comunicações, o desempenho das atividades *cyber* eletromagnéticas, no que tange à proteção, ao monitoramento e ao ataque.

Tal responsabilidade atribui, à “Arma do Comando”, uma mudança significativa de seu emprego nos conflitos modernos: assumir papel preponderante na resolução dos conflitos; podendo, por meio de ataques no espaço *cyber* eletromagnético, paralisar toda a estrutura produtiva, financeira e de defesa de um outro Estado; inviabilizar o desdobramento, no teatro de operações, de suas forças; e impedir o conflito, antes mesmo do primeiro disparo de uma arma de fogo.

Conclui-se, portanto, que a Arma de Comunicações, no entendimento deste autor, deve ser vista com outros olhos, pelo Alto Comando do Exército, num primeiro momento; e pelo Ministério da Defesa, em uma fase posterior, quando se pensa nas Forças Armadas como um todo e na necessidade de interoperabilidade, entre a Marinha, o Exército e a Força Aérea.

REFERÊNCIAS

-*ADEE, Sally.* ***The hunt for the kill switch****. IEEE Spectrum*, v. 45, n. 5, p. 34-39, 2008;

-AMARANTE, José Carlos A. (2010), **"A Batalha Automatizada: um sonho possível?"** Cadernos de Estudos Estratégicos, Vol. 09, pp. 03 -19;

-ARQUILLA, J. R. ***Cyberwar is coming*****!** Santa Monica: *Rand Corporation*.1993;

-BARRETO, Rafael José Vieira - **Análise comparativa da liderança militar e empresarial no contexto do mundo VUCA: desafios e oportunidades**./ Rafael José Vieira Barreto.—2019;

-BISHARA, M. ***Um Inimigo Difuso***. *Le Monde Diplomatique* Brasil. Disponível em:<http://www.diplomatique.org.br/acervo.php?id=358>. Acesso em: 16 julho 2015;

- BRASIL. Ministério do Exército. Manual de Campanha C11-1. **Emprego das Comunicações**. 2. ed. Brasília, 1997.

- BRASIL. Ministério da Defesa. Manual MD31-P-01. **Política para o Sistema Militar de comando e Controle**. Brasília, 2001.

- BRASIL. Decreto n. 5.484, de 30 de junho de 2005. **Aprova a Política de Defesa Nacional, e dá outras providências**. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 1 jul. 2005.

- BRASIL. ***Estratégia Nacional de Defesa****.* Brasília: Ministério da Defesa, 2008.

-BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. ***Livro Verde: segurança cibernética no Brasil*****.** Claudia Canongia e Raphael Mandarino Júnior (org.). Brasília: GSIPR/SE/DSCI, 2010.

- BRASIL. Presidência da República. Secretaria de Assuntos Estratégicos. ***Desafios estratégicos para segurança e defesa cibernética.*** Organizadores: Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. Brasília, 2011

- BRASIL. Comandante do Exército. Portaria nº. 666, de 4 de agosto de 2010. **Cria o Centro de Defesa Cibernética do Exército e dá outras providências**. *Boletim do Exército*, n. 31, de 6 de agosto de 2010. Site DefesaNet 2011.

- BRASIL. Escola de Comando e Estado-Maior do Exército. **Manual de Elaboração de Projetos de Pesquisa na ECEME**. Rio de Janeiro, 2012.

- BRASIL. Exército Brasileiro. EB20-C-07.001 - **Catálogo de Capacidades**. Brasília. 2013.

- BRASIL. Ministério da Defesa. Exército Brasileiro. Estado Maior do Exército. **Operações de Informações**. 1. Ed. Brasília. 2014.

- BRASIL. Exército Brasileiro. Manual EB20-MF-10.101. **O Exército Brasileiro**. 1. ed. Brasília, 2014.

- BRASIL. Ministério da Defesa. **Doutrina para o Sistema Militar de Comando e Controle**. 1. ed. Brasília, 2015.

- BRASIL. Exército Brasileiro. Manual de Campanha EB20-MC-10.205. **Comando e Controle**. 1.ed. Brasília. 2015.

- BRASIL. Exército Brasileiro. Portaria nº 197-EME, de 26 de setembro de 2013. **Concepções e conceitos doutrinários com vistas à incorporação, na Força Terrestre, das capacidades e das competências necessárias ao seu emprego na Era do Conhecimento**. Brasília.2015.

- BRASIL. Ministério da Defesa. Estado-Maior de Defesa. MD35-G-01, **Glossário das Forças Armadas**. 5. Ed. Brasília, DF. 2015.

- BRASIL. Ministério da Defesa. MD31-M-03/2015. **Doutrina para o Sistema Militar de Comando e Controle**. 3.Ed Brasília, DF. 2015.

- BRASIL. Estado-Maior do Exército. **Manual de Comando e Controle**. 1. ed. Brasília, 2015.

- BRASIL, Ministério da defesa. MD 31-S-02: **Conceito de Operações do Sistema Militar de Comando e Controle**. 1ª edição. Brasília 2016.

- BRASIL. Exército Brasileiro. Manual de Campanha EB70-MC-10.341. **Lista de Tarefas Funcionais**. 1. ed. Brasília, 2016.

- BRASIL. Exército Brasileiro. Manual EB70-MC-10.223. **Operações**. 5. ed. Brasília, 2017.

- BRASIL. Ministério da Defesa. Exército Brasileiro. **Comando de Operações Terrestres**. EB70-MC-10.232, Guerra Cibernética. 1. Ed. Brasília, DF. 2017.

- BRASIL. Exército Brasileiro. Manual de Campanha EB70-MC-10.241. **As Comunicações na Força Terrestre**. 1. ed. Brasília. 2018.

- BRASIL. EB20-MF-10.102: **Fundamentos Doutrina Militar Terrestre**. Brasília, 2019.

- BRASIL. Exército Brasileiro. Manual de Campanha EB70-MC-10.201. **A Guerra Eletrônica na Força Terrestre**. 1.ed. Brasília, 2019.

- BRASIL. EB70-MC 10.246: **As Comunicações nas Operações.** Brasília, 2020.

-BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. EB70-MC-10.247: **A Guerra Eletrônica nas Operações**. 1. Ed. Brasília, DF. 2020.

- BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. C 34-1 **Emprego da Guerra Eletrônica**. 2. Ed. Brasília, DF. 2009.

- CARVALHO, L.O.M. D et al. **SIPLOM 3: A Terceira Geração do Sistema de Comando e Controle da Defesa**. Rio de Janeiro 2018.

- *CLARK, Blane* R. **As Operações de Informações como um Elemento Dissuasório do Conflito Armado**. Militar *Review.* Ed. Brasileira, p. 57-65. Set-Out 2010.

- *CLARK, Richard A.; KNAKE, Robert K. Cyber War:* ***The next threat to national security and what to do about it****. New York*: Ecco, 2010.

- *FALLIERE*, Nicolas; *MURCHU, Liam* O.; *CHIEN*, Eric. W32. ***Stuxnet dossier. White paper, Symantec Corp****., Security Response*, v. 5, n. 6, p. 29, 2011.

- GONTIJO, S. **O Livro de Ouro da Comunicação**. Rio de Janeiro: Ediouro, 2004.

- HAMMES, T. X. **A Guerra de Quarta Geração Evolui, A Quinta Emerge.** Military Review (edição brasileira), p. 16-27, set/out. 2007.

- JOHNSON, Robert A. **Prevendo a Guerra do Futuro.** Doutrina Militar Terrestre em Revista, p. 68-82, ed. 006, 2014.

- *KAISER, Robert.* ***The birth of cyberwar. Political Geography***, v. 46, p. 11-20, 2015.

- *KEITH, B. Alexander*. **A Guerra no ambiente cibernético***.* Washington D.C.: *National Defense University Press, Joint Force Quarterly, MILITARY Technology* (MILTEC), mar. 2011. p. 41-44.

- MARQUES, Rafael Siqueira. **A Evolução dos Conflitos Assimétricos e suas Consequências no Preparo e Emprego das Forças Armadas: os projetos estratégicos do Exército Brasileiro e a implementação da defesa cibernética.** Artigo apresentado como requisito parcial para a obtenção do título de Especialista em Relações Internacionais pela Universidade de Brasília. Brasília.2015

- MANDARINO JR., Raphael. ***Segurança e Defesa do Espaço Cibernético Brasileiro.*** Brasília, 2010.

- *METZ, Steven.* ***Strategic Asymmetry****. Military Review*, p. 23-31, Jul./Aug. 2001.

- *NYE, J. S.* ***Power and interdependence***. 3 ed. New York: *Longman*, 2001.

- NETO, Samuel Bombassaro. **A atuação da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente em operações ofensivas**. ECEME. Rio de Janeiro, 2018.

-NOBREGA, Gildenildo Paulino. **Os Sistemas Militares de Comando e Controle do Exército Brasileiro nas Operações**. Rio de Janeiro. 2019.

- PINHEIRO, Fábio Ponte. ***A Cibernética como arma de combate***. Rio de Janeiro: Escola Superior de Guerra, 2013.

- *REED, Thomas.* ***At the Abyss: An Insider's History of the Cold War***. Presidio Press. 2005;

- *RICHARDSON, Doug*. **Guerra eletrônica: guia das armas de guerra**. Nova Cultural. São Paulo. Dez/1991.

- SANTOS, Gabriel Augusto. **"Novo Ano, Novos Desafios: Ciberataques e Ciberdefesas".** Revista Militar. nº 2496, janeiro de 2010. Disponível em: http://www.revistamilitar.pt/artigo.php?art_id=533. Acessado em junho de 2015.

- SANTOS, *Michell* Medeiros – **Convergência entre atividades de Guerra Cibernética e Guerra Eletrônica no 1° Batalhão de Guerra Eletrônica nas Operações** - EsAO 2020

- *SARSFIELD, Thomas.* ***Information War 2022: Musings of a Senior Officer on Russian Information Warfare and Recent Events****. Military Review*, 2019.

- *SHAKARIAN*, Paulo. ***The* 2008 *Russian cyber campaign against Georgia****. Military review*, v. 91, n. 6, p. 63, 2011.

- SILVA, Gilmar Pereira. **Guerra Cibernética: preparo e emprego do Exército**. Rio de Janeiro, 2006, 46 f.

- *UNITED STATES. Headquarters. Department of the Army. FM 3-12,* ***Cyber Space and Electronic Warfare Operations***. Apr, 2014.

-- VERGARA, S. C. **Métodos de pesquisa em administração**. 3ª Ed. São Paulo: Atlas, 2008. 287 p., il. Bibliografia: p. 269-287. ISBN: 978-85-224-4999-6.

- VISACRO, Alexandre. Superando o Caos. **A Função de Combate Comando e Controle Além da Tecnologia da Informação.** Military Review, Kansas, EUA, Tomo 70, Número 4, p. 70-88, julho-agosto. 2015.

- VISACRO, A. **A Guerra na Era da Informação**. 1 Ed. São Paulo, Contexto, 2018.

- *WEBB, D. C.* ***ECHELON and the NSA.*** In: *COLARIK, A. M.; JANCZEWSKI, L. J.* ***Cyber warfare and cyber terrorism****.* Nova Iorque, EUA: *Information Science Reference*, 2008.

- WWW.CCOMGEX.EB.MIL.BR. **Estrutura Organizacional da GE no Exército Brasileiro.** Disponível em: http://www.ccomgex.eb.mil.br/dpdg/arquivos/CCOMGEX .pdf/. Acesso em 12 Agosto2021;

-WWW.DEFESACIBERNÉTICA.IME.EB.BR. **Sistema Brasileiro de Defesa Cibernética**. Disponível em: http://www.defesacibernetica.ime.eb.br/Acesso em 12 Agosto 2021.

-WWW.DEFESA.GOV. BR. **Estratégia Nacional de Defesa**. Disponível em: <http:// www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf>. Acesso em: 22/06/2021.

-WWW.DEFESA.GOV. BR. **Doutrina Militar de Defesa**. Disponível em:<https:// www.defesa.gov.br/index.php/ doutrina-militar.htm>. Acesso em 22/06/2021.

- WWW.PODER360.COM.BR. **Brasil é o país onde há mais preocupação com fake News.** Disponível em https://www.poder360.com.br/midia/brasil-e-o-pais-onde-há-mais-preocupação-com-fake-news/Acesso em 12 Ago2021;

- WWW. *ENIGMASSOFTWARE*.COM. **Gráfico por incidência de Cyber crime no mundo no mundo**. Disponível em: https://www.enigmasoftware.com/pt/20-paises-maior-indice-crimes-ciberneticos/ Acesso em 12 Ago 2021.

- *ZETTER, Kim. Countdown to Zero Day:* ***Stuxnet and the launch of the world's first digital weapon****. Broadway books*, 2014.