ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM MARCELO JOSÉ MARQUEZ DE CAMPOS

A UTILIZAÇÃO DA INFRAESTRUTURA DE REDE DE COMUNICAÇÕES EXISTENTE NO EXÉRCITO BRASILEIRO PARA AS OPERAÇÕES DE GUERRA ELETRÔNICA

Rio de Janeiro
2021

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM MARCELO JOSÉ MARQUEZ DE CAMPOS

A UTILIZAÇÃO DA INFRAESTRUTURA DE REDE DE COMUNICAÇÕES EXISTENTE NO EXÉRCITO BRASILEIRO PARA AS OPERAÇÕES DE GUERRA ELETRÔNICA

Trabalho de Conclusão de Curso apresentado à Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do grau especialização em Ciências Militares
Orientador: Cap Com Rodolfo de Azevedo Maymone

Rio de Janeiro
2021

INFORMAÇÃO DE P&D – ACESSO RESTRITO
§1º do Art. 7º da Lei nº 12.527, de 18 de novembro de 2012
Inciso II do Art. 6º do Decreto nº 7.724, de 16 de maio de 2012

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

DIVISÃO DE ENSINO / SEÇÃO DE PÓS-GRADUAÇÃO

FOLHA DE APROVAÇÃO

Autor: **Cap Com MARCELO JOSÉ MARQUEZ DE CAMPOS**

Título: **A UTILIZAÇÃO DA INFRAESTRUTURA DE REDE DE COMUNICAÇÕES EXISTENTE NO EXÉRCITO BRASILEIRO PARA AS OPERAÇÕES DE GUERRA ELETRÔNICA.**

Trabalho Acadêmico, apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito parcial para a obtenção da especialização em Ciências Militares.

APROVADO EM _____/_____/_____ *CONCEITO:* _____

BANCA EXAMINADORA

Membro	**Menção Atribuída**
_____ **CARLOS ANDRÉ DOS SANTOS MEIRELLES DE ANDRADE - Maj** Cmt Curso e Presidente da Comissão	
_____ **RODOLFO AZEVEDO MAYMONE - Cap** 1º Membro e Orientador	
_____ **GLAUCO GONÇALVES DA SILVA - Cap** 2º Membro	

_____
MARCELO JOSÉ MARQUEZ DE CAMPOS – Cap
Aluno

SUMÁRIO

RESUMO

O presente trabalho tem por finalidade apresentar a infraestrutura de rede de comunicações existente no Exército Brasileiro, no caso, a EBNet, a fim de que possa servir de apoio para as operações de Guerra Eletrônica (GE), tanto para o acesso remoto aos equipamentos de GE, quanto para o Centro de Operações de Guerra Eletrônica (COGE).

Palavras-Chave: EBNet, Guerra Eletrônica, COGE

ABSTRACT

The present work aims to present the existing communications network infrastructure in the Brazilian Army, in this case, EBNet, so that it can serve as support for Electronic Warfare (EW) operations, both for remote access to equipment of EW, as well as the Electronic Warfare Operations Center (COGE).

Key–Words: EBNet, Eletronic Warfare, COGE

1.INTRODUÇÃO

Nos últimos dez anos, as Forças Armadas (FA) vem participando na segurança interna do nosso país, seja em Operações de Garantia da Lei e da Ordem (GLO), seja atuando como Poder de Polícia no combate a crimes transfronteiriços. Devido a isso, o Exército Brasileiro (EB) vem conseguindo, de certa maneira, se adestrar em virtude dessas operações que podem vir a surgir de experiência em diversas operações de GLO, onde a Guerra Eletrônica (GE) teve que atuar, sendo fundamental no apoio à informação como fonte de sinais, utilizando da rede corporativa do Exército Brasileiro para conseguir acesso aos equipamentos de GE, bem como receber essas informações para o Centro de Operações de Guerra Eletrônica.

1.1 PROBLEMA

Na última década, o Brasil recebeu Grades Eventos como: Jogos Mundiais Militares (2011), Jornada Mundial de Jovens (2012), Rio +20 (2012), Copa América (2013), Copa do Mundo (2014), Jogos Olímpicos e Paraolímpicos (2016) e também ocorreram operações de pacificação, bem como GLO, as quais foram Op Arcanjo (2010), Op São Francisco (2014), Op Capixaba (2017), Op Potiguar II (2017), Op Potiguar III (2018), Intervenção Federal (2017), fazendo com que as FA adestrassem suas tropas para esses tipos de eventos/conflitos, o que pode colocar sua doutrina em prática.

O uso da Guerra Eletrônica (GE) pelo Exército Brasileiro nessas operações teve um caráter decisivo, onde o processamento dos dados obtidos pelos sensores de GE, realizada no COGE, dava uma melhor consciência situacional do Teatro de Operações (TO). O COGE, segundo o manual a Guerra Eletrônica nas Operações (EB70–MC–10.247), deve oferecer possibilidade de ligações com os escalões superiores apoiados. (BRASIL, 2020, p.2-6)

Segundo o manual de campanha A Guerra Eletrônica na Força Terrestre (EB70-MC-10.201), existem os princípios de flexibilidade e oportunidade da GE os quais pretendem melhorar o fluxo de informações, dar consciência situacional e um melhor redirecionamento para o esforço dos sensores de sinais, a partir dos dados obtidos. (BRASIL,2019,p.2-13 e 2-14)

Face o exposto, como a infraestrutura de rede de comunicações do Exército Brasileiro pode contribuir para uma difusão rápida da informação, sendo um meio de comunicações importante para a utilização modular dos meios de GE, bem como do recebimento dessas informações pelo COGE?

1.2 OBJETIVOS

1.2.1 Objetivo geral

O objetivo dessa pesquisa é de verificar a possibilidade de utilizar-se da infraestrutura de rede de comunicações existente no Exército Brasileiro para as operações de Guerra Eletrônica, em operações de Não Guerra.

1.2.2 Objetivos específicos

Para atingirmos tal objetivo, serão abordados os seguintes aspectos:

a) Apresentar a rede interna do Exército Brasileiro;

b) Discutir a eficácia dos meios de Guerra Eletrônica de forma remota a partir dos Centros de Operações de Guerra Eletrônica;

1.3 JUSTIFICATIVAS

Durante as diversas operações de Garantia da Lei e da Ordem executadas dentro do território nacional nos últimos anos, o 1º Batalhão de Guerra Eletrônica foi bastante solicitado para atuar, utilizando a sua doutrina para produção de conhecimento a respeito dos alvos designados. Nas operações Arcanjo (2010- 2012), São Francisco (2014-2015), Capixaba (2017), Potiguar II (2017), Potiguar III (2018) e Furacão (2017-2018) além dos eventos mundiais como Rio +20 (2012), Jornada Mundial da Juventude (2012), Copa América (2013), Copa do Mundo (2014), Jogos Olímpicos e Paralímpicos Rio 2016 e Reunião de Cúpula dos Brics (2014 e 2019), o Centro de Operações de Guerra Eletrônica, do 1º Batalhão de Guerra Eletrônica, esteve, segundo em sua doutrina, justaposto ao comando da operação, tendo seu campo de atuação limitado ao uso de suas antenas para links-rádio. A relevância maior seria o uso

de uma rede segura, no caso, a rede corporativa do Exército (EBNet) em proveito das ações de Guerra Eletrônica, seja na operação remota, seja no posicionamento do COGE, ganhando rapidez, fluidez e objetividade durante o fluxo de informações transmitidas durante as operações.

2. METODOLOGIA

2.1 OBJETO FORMAL DE ESTUDO

Verificar a possibilidade do uso da rede corporativa do Exército Brasileiro (EBNet) para o desempenho das ações de Guerra Eletrônica.

2.2 AMOSTRA

Foram escolhidos para responder um questionário alguns militares com experiência em operações de GLO/Inteligência e ex-integrantes do 1º BGE, possuidores do Curso Básico de Guerra Eletrônica, que participaram nessas operações, conforme tabela que se segue abaixo:

NOME	JUSTIFICATIVA
ALLAN PAULO ALVARENGA SANTOS Maj COM	Op Arcanjo (2010/2012) - Complexo do Alemão/ Rio de Janeiro -RJ Op São Francisco (2014/2015) – Complexo da Maré/ Rio de Janeiro - RJ Copa do Mundo (2014) – Rio de Janeiro - RJ Intervenção Federal (2017/2018) – Rio de Janeiro - RJ
MICHELL MEDEIROS SANTOS Cap COM	Op Arcanjo (2010/2012) - Complexo do Alemão/ Rio de Janeiro -RJ

	Op São Francisco (2014/2015) – Complexo da Maré/ Rio de Janeiro - RJ Copa do Mundo (2014) – Salvador - BA Intervenção Federal (2017/2018) – Rio de Janeiro - RJ
THYAGO HENRIQUE ALMEIDA SIMÕES Cap COM	Op São Francisco (2014/2015) – Complexo da Maré/ Rio de Janeiro - RJ Olimpíadas (2016) – Rio de Janeiro - RJ Intervenção Federal (2017/2018) – Rio de Janeiro - RJ
GABRIEL CARNEIRO DE **CASTRO** Cap COM	Op São Francisco (2014/2015) – Complexo da Maré/ Rio de Janeiro - RJ Olimpíadas (2016) – Rio de Janeiro - RJ Intervenção Federal (2017/2018) – Rio de Janeiro - RJ

Tabela Nr 1: Operações participadas por ex-integrantes do 1º BGE

Fonte: o autor, baseado no questionário

2.3 DELINEAMENTO DA PESQUISA

A pesquisa está delineada através dos manuais que demonstram de forma dedutiva a doutrina da Guerra Eletrônica quanto a sua forma de atuação. Com o advindo da rede corporativa do Exército, a EBNet, foram descritas outras formas de atuação da Guerra Eletrônica, e o que isso está gerando de ganho para o aprimoramento tático-operacional.

2.3.1 Procedimentos para revisão da literatura

Primeiramente foi feita uma pesquisa bibliográfica em todos os manuais nacionais de Guerra Eletrônica, Inteligência Militar, Doutrina Militar Terrestre do Exército Brasileiro e de Gestão de Riscos, depois comparado com manuais de Guerra Eletrônica e Inteligência do Exército Americano para verificar se a doutrina deles era similar a nossa.

2.3.2 Procedimentos Metodológicos

Foram pesquisados os manuais de Guerra Eletrônica, para que fossem descritas a doutrina do Exército Brasileiro, artigos, palestras e revistas sobre a rede corporativa do Exército, a EBNet, bem como os manuais de inteligência. Após isso, foram selecionados alguns militares, já citados, com experiência em Guerra Eletrônica para responderem a um questionário a fim de contribuírem com os benefícios do uso da EBNet nas operações de Guerra Eletrônica.

2.3.3 Análise dos Dados

A partir da pesquisa dos diversos manuais de Guerra Eletrônica, foram comparados com doutrina militar do Exército dos Estados Unidos da América, para que se possam analisar as variáveis através desses conceitos. Além disso, iremos verificar as respostas ao questionário dos militares selecionados a fim de confirmamos se a doutrina está sendo realizada na prática.

3. REFERENCIAL TEÓRICO

3.1. Operações

Segundo o Manual de Fundamentos de Operações,

> o Espaço de Batalha é, portanto, a dimensão física e virtual onde ocorrem e repercutem os combates, abrangendo as expressões política, econômica, militar, científico-tecnológica e psicossocial do poder, que interagem entre si e entre os beligerantes. Compreende todas as dimensões, tangíveis e intangíveis, nas quais o comandante deve aplicar o seu Poder de Combate. O Campo de Batalha está incluído no Espaço de Batalha. (BRASIL,2014,p.2-7):

A figura abaixo mostra um exemplo dessas áreas:

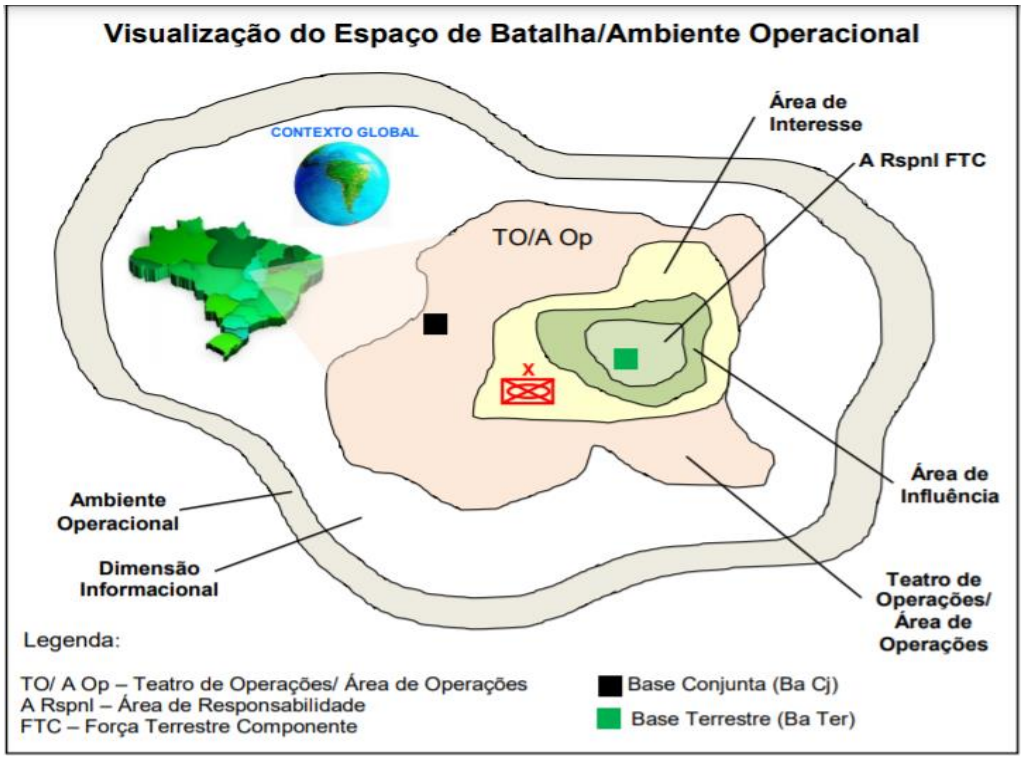

Figura 1: Visualizando o Espaço de Batalha/Ambiente Operacional

Fonte: Manual de Fundamentos Operações – EB20-MF-10.103

Segundo o Manual de Fundamentos de Operações, também os aspectos informacionais, espectro eletromagnético e fatores relacionados ao espaço cibernético são considerados dimensões intangíveis do Espaço de Batalha. (BRASIL,2014,p.2-7) Nesse aspecto, independe de onde se esteja operando, embora os sensores de sinais devam estar próximos aos alvos de interesse.

O Manual de Fundamentos de Operações cita que:

> A Superioridade de Informações é traduzida por uma vantagem operativa derivada da habilidade de coletar, processar, disseminar, explorar e proteger um fluxo ininterrupto de informações aos comandantes em todos os níveis, ao mesmo tempo em que se busca tirar proveito das informações do oponente e/ou negar-lhe essas habilidades. É possuir mais e melhores informações do que o adversário sobre o ambiente operacional. Permite o controle da dimensão informacional (espectros eletromagnético, cibernético e outros) por determinado tempo e lugar. (BRASIL,2014,p.2-7)

Esse apoio a decisão, em tempo oportuno, facilita em muito as tomadas de linhas de ação de forma precisa e rápida para o sucesso da operação. Segundo o manual Fundamento de Operações, as operações militares do Exército

Brasileiro dividem-se em Operações de Guerra e Operações de Não Guerra, devido aos procedimentos e princípios utilizados.

As Operações de Guerra, segundo o Manual de Fundamentos de Operações (BRASIL,2014,p.2-9):

> [..] utilizam o Poder Militar, explorando a plenitude de suas características de emprego da força, ou seja, a violência militar em sua maior expressão. Nelas empregam-se todas as capacidades das organizações operativas das Forças Armadas, ou ameaça fazê-lo, aplicando os princípios e procedimentos de combate derivados da arte da guerra.

Já as Operações de Não Guerra, segundo o Manual de Fundamentos de Operações (BRASIL,2014,p.2-9),é citado da seguinte forma:

> Em situações de paz (estável ou instável) ou de crises, empregam-se, entre outras medidas, as de caráter militar, mediante o uso de forças militares com a aplicação de parte de suas capacidades, para evitar a escalada da crise ou anular a possibilidade de realização de campanhas e operações militares de guerra de vulto. Realizam-se, também, em apoio às autoridades governamentais (nacionais ou internacionais).

A diferença básica entre as duas características de operações é a quantidade de capacidades utilizadas, bem como a sua aplicação. Após mostrarmos os conceitos básicos de Operações, bem como suas divisões por zonas de atuação e suas características quanto aos procedimentos e princípios utilizados, falaremos sobre a rede de comunicações nas Operações de Guerra e Não Guerra.

3.1.1. As Redes de Comunicações em Operações de Guerra

Segundo CAMILO et al.(2020), as operações de guerra estão afastadas das organizações militares. Para que ocorra o uso dos sistemas do EB:

> Os comandantes dos elementos, tais como brigadas e batalhões, da FTC desdobrados são conectados, através de enlaces de HCLOS (*High-Capacity Line-Of-Sight* ou Linha de Visada de Alta Capacidade) providos pelo MTO (Módulo de Telemática Operacional) do EB, com a rede do comando da operação, o que provê

> conectividade uns com os outros e com a estrutura de acompanhamento. (CAMILO et al,2020,p.8)

Ainda, o autor, no mesmo artigo cita também que todos os equipamentos usados possuem capacidade de comunicações utilizando protocolo IP (Internet Protocol). A figura abaixo mostra como seria realizado esses enlaces:

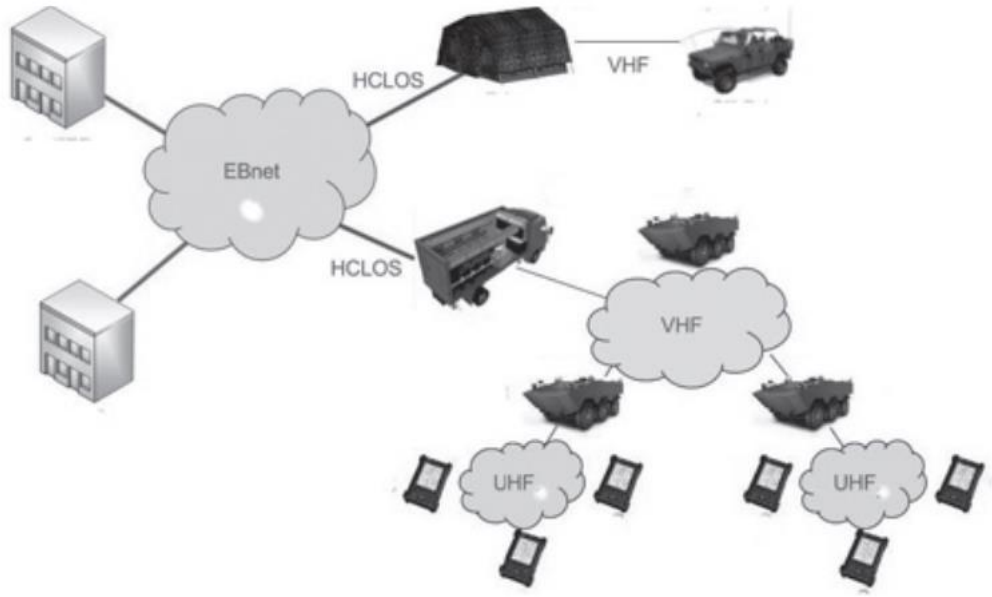

Figura 2: Rede de comunicações em Operações de Guerra
Fonte: CAMILO et al.(2020),p.8

3.1.2. As Redes de Comunicações em Operações de Não Guerra

Segundo Camilo et al.(2020), este mostra as redes de comunicações em operações de não guerra onde:

> Os militares que ficam em posições fixas utilizam amplamente redes infraestruturadas de alta capacidade, como a EBNet ou a ROD (Rede Operacional de Defesa), rede segregada, estabelecida pela MD, que proporciona grande segurança para o fluxo de informações necessário à condução de operações conjuntas e propicia interoperabilidade às FFAA brasileiras. Estas redes são os pontos de conectividade com os militares que circulam por uma área urbana pré-determinada os quais trafegam suas informações através de rede celular. Os militares em posições afastadas, para defender uma estrutura estratégica, são conectados à estrutura principal do sistema através de enlace de HCLOS. (CAMILO et al,2020,p.8)

A figura abaixo mostra como seria esse cenário:

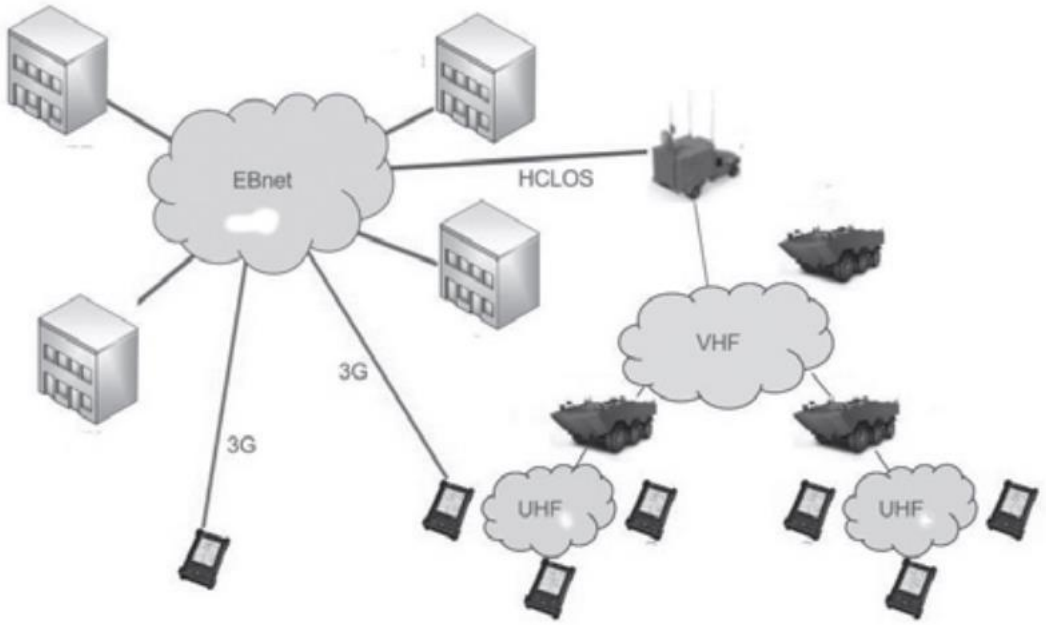

Figura 3: Rede de comunicações em Operações de Não Guerra
Fonte: CAMILO et al.(2020),p.8

O ponto chave nos tipos de operações se dá pela capacidade de seus equipamentos, os quais possuem conectividade IP, onde podem se ligar através de links físicos ou de dados à EBNet, transmitindo as informações com segurança.

O manual Operation Urban FM 3-06, do Exército dos Estados Unidos da América, cita que na Função de Combate Comando e Controle:

> The C2 system faces difficulties placed on the tactical Internet and system hardware by the urban environment, by the increased volume of information, and by requirements to support the dynamic decision making necessary to execute successful UO. (EUA,2006,p.4-13)

Isso mostra a dificuldade de operar em um ambiente urbano face à Internet tática e os sistemas dos equipamentos, acrescidos do fluxo de informações para uma tomada de decisão precisa.

> Sobre os Sistemas de Informações, o manual Operation Urban FM3-06, diz que:Urban structures, materials, densities, and configurations (such as urban canyons) and power

> constraints associated with man-portable radios significantly degrade frequency modulation (FM) communications. (EUA,2006,p.4-15)

Para mitigar os problemas advindos de áreas urbanas, o manual nos mostra algumas tarefas a serem cumpridas como a colocação de mais postos de comunicações, bem como retirar as demandas das comunicações, como mostra a figura abaixo:

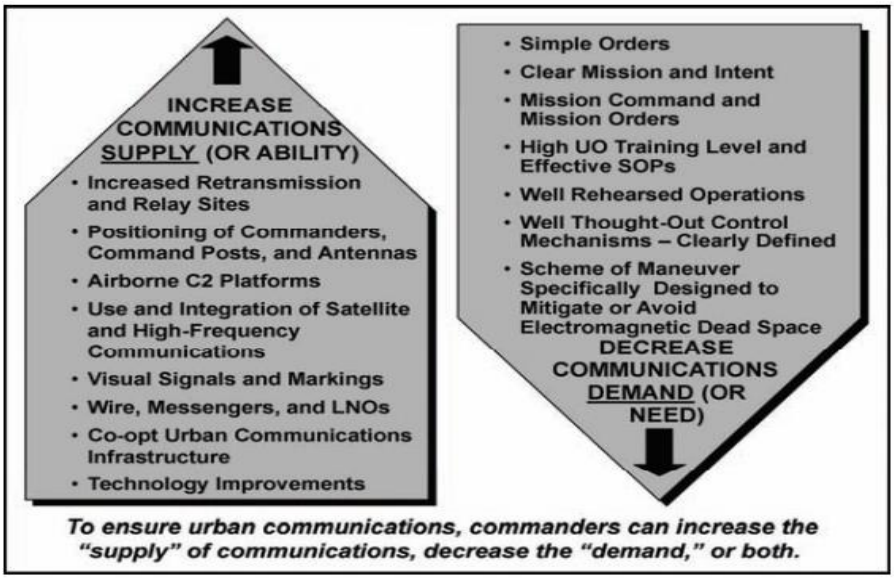

Figura 4: Métodos para cobrir os problemas com comunicações

Fonte: Manual Operation Urban – FM 3-06(EUA,2006,p.4-16)

Uma dessas tarefas seriam de incrementar repetidoras, plataformas C2 para aeronaves, usufruir das infraestrururas de comunicações existentes nas cidades (backbones).

A partir do que foi apresentado até agora, podemos observar que as comunicações, seja em Operações de Guerra ou de Não Guerra, necessitam de infraestrutura que irão ser criadas ou apropriadas para seu estabelecimento em proveito das ações. Para que isso seja realizado por uma rede segura, onde as informações possam ser transitadas, mesmo que com um nível maior de segurança, uma sugestão seria da utilização da rede corporativa do Exército Brasileiro, a EBNet.

3.2. Sistema de Telemática do Exército (SisTEx)

O SisTEx, segundo o site do CITEx, consiste no conjunto formado pelo Centro Integrado de Telemática do Exército (CITEx) e pelas suas Organizações Militares diretamente subordinadas, os Centros de Telemática de Área (CTA) e

Centros de Telemática (CT), e pelo Destacamento Técnico de Tecnologia da Informação (DTTI) em Santa Maria/RS, situados nas guarnições dos Comandos de Regiões Militares, às quais prestam o apoio de Telemática. Os CTA apoiam, também, os Comandos Militares de Área de sua região.

Durante a palestra proferida ao CCOM ESAO, pelo SubChefe do CITEx, foi apresentado que o SisTEx integra o Sistema de Comando e Controle do Exército (SC²Ex), o qual possui duas vertentes, o Sistema Estratégico de Comando e Controle do Exército (SEC²Ex) e o Sistema de Comando e Controle da Força Terrestre (SC²FTer), onde os dois dependem e devem trabalhar juntos em prol das operações militares a fim de garantir o Comando e Controle, tal qual é representada pela imagem abaixo:

Figura 5: Vertentes do SC²Ex
Fonte: Palestra ao PCI CCOM ESAO 2021 pelo CITEx

3.2.1 Atribuições do SisTEx

O Sistema de Telemática do Exército realiza basicamente as seguintes funções: conectividade, hospedagem em nuvem, proteção cibernética e serviços de TI. A conectividade seria o acesso as Organizações Militares (OM) através da EBNet com links de dados, estações satelitais, VPNs, fibra ótica através das OMs diretamente subordinadas ao CITEx como veremos na figura a seguir:

Figura 6: OMDS do CITEx

Fonte: Palestra ministrada no PCI CCOM ESAO 2021 pelo CITEx

Além de Santa Maria, a qual possui um Destacamento:

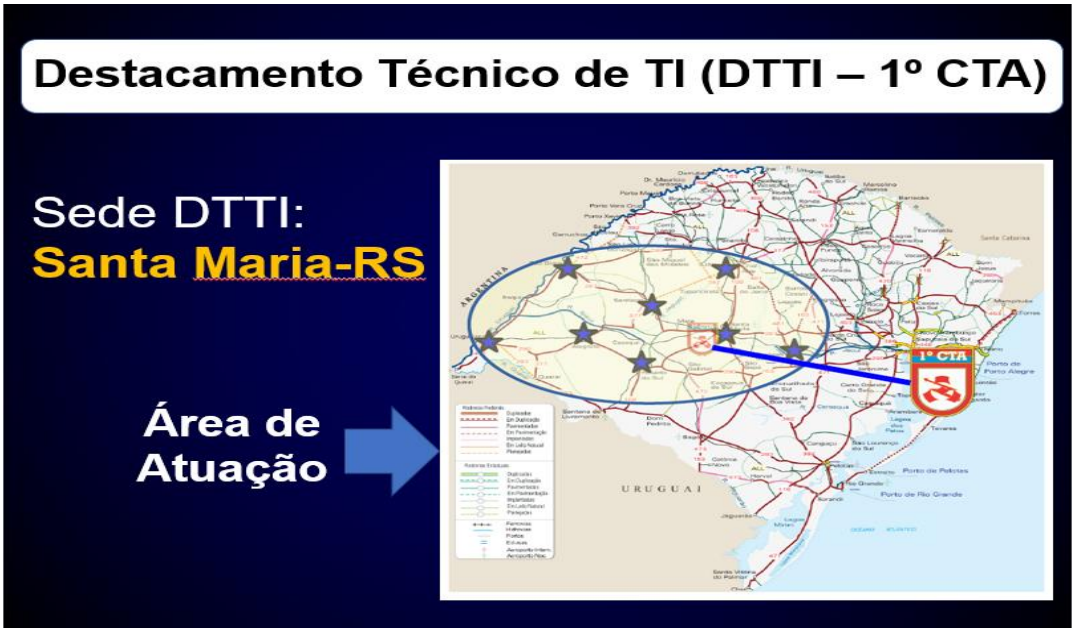

Figura 7: Único destacamento técnico de TI

Fonte: Palestra ministrada no PCI CCOM ESAO 2021 pelo CITEx

Essas OMDS, mais o Destacamento Técnico de TI, nos conferem apoio para as diversas operações em que se precise do uso dos equipamentos na rede EBNet. Para ser ter uma noção da dimensão da rede corporativa, nos foi apresentado que são 65000 estações de trabalho, 950 conectividades em 656

Organizações Militares. Esse somatório de estações de trabalho se multiplica quando associamos equipamentos e computadores durantes as operações, aumentando mais ainda o trabalho de todo o SisTEx.

Um outro dado interessante são os backbones regionais, que as saídas por onde a EBNet é distribuída, os quais ajudam efetivamente aos militares que desejam usufruir da rede corporativa do Exército, como veremos na figura abaixo:

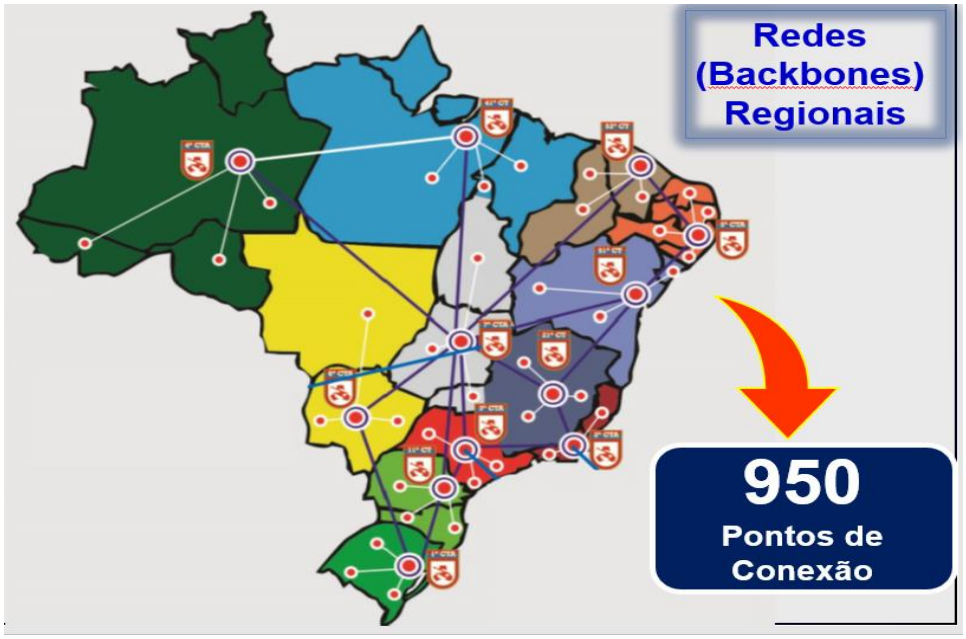

Figura 8: Redes (backbones) regionais

Fonte: Palestra ministrada no PCI CCOM ESAO 2021 pelo CITEx

Quanto a essas funcionalidades, os CT/CTA possuem seus catálogos de serviços próprio, onde oferecem os serviços de Dados, Internet Corporativa, VOIP e Vídeoconferência. A Internet, como citada anteriormente no manual de Operações Urbanas, deve ser usada a que o Exército Brasileiro fornece, pois é nela que se tem todos os controles de segurança a vista dos CTA. Caso venhamos a contratar Internet para as operações com provedores que não tenha uma preocupação com a segurança, podemos incorrer em ataques cibernéticos vindo a comprometer todo o SisTEx. Uma outra funcionalidade importante, atualmente, é a de armazenar os diversos sistemas, o qual o CITEx possui um serviço de hospedagem bem amplo, com 14 DATA Centers conseguindo hospedar 1100 sistemas, 2600 máquinas virtuais, 460 servidores físicos, com uma capacidade num total de 4 Petabytes.

O Data Center central está localizado no Centro Integrado de Telemática do Exército (CITEx), hospedando a Rede Corporativa EBNet. Outro dado de interesse é de que os Sistemas Corporativos são armazenados no Data Center do Exército Brasileiro, com responsabilidade de desenvolvimento e manutenção pelo Centro de Defesa de Sistemas, bem como os Sistemas Regionais que são armazendos no Data Center do CT/CTA, com responsabilidade de desenvolvimento e manutenção pelo Centro de Defesa de Sistemas.

Como podemos observar, o SisTEx serviços excepcionais para utilização da rede corporativa do Exército Brasileiro. Com isso, a partir da compra de equipamentos de Guerra Eletrônica com comunicação de protocolo IP, nos deu um pensamento para utilizar a rede EBNet em proveito das ações de GE.

Durante a Operação São Francisco (2014-2015), realizada no Complexo da Maré, na cidade do Rio de Janeiro – RJ, bem como na Operação Arcanjo (2010-2012), havia um Destacamento de Guerra Eletrônica atuando em prol da Operação. Nessas oportunidades, os meios de comunicações utilizados foram sempre de dados, através de links PTP, dos sensores de sinais até o Centro de Operações Guerra Eletrônica (COGE). Essas duas operações tiveram como características uma área definida do teatro de operações, o que facilitava dispor somente desses meios para conexão entre os sensores e o COGE. Podemos ver isso na figura Nr 9 abaixo:

Figura 9: Desdobramento do sistema MAGE na Operação São Francisco

Fonte: o autor, baseado em relatórios da operação

Durante o Reconhecimento para os Jogos Olímpicos e Paraolímpicos 2016, foram definidas 04 (quatro) grandes áreas chamados Comandos de Defesa Setoriais (CDS) em Copacabana, Maracanã, Deodoro e Barra da Tijuca. Igual as Operações anteriormente citadas, havia, também, uma área bem definida de atuação. No reconhecimento, foi visto que o 2º Centro de Telemática de Área (2º CTA) possuía links, via rádio, onde se trafegava a EBNet para os quartéis do Comando Militar do Leste. A partir daí, começou-se o pensamento de utilizar a rede corporativa do Exército para ter acesso aos dados obtidos pelos sensores de sinais, bem como o fluxo dessas informações com o COGE.

Em 2017, deflagrou-se a Intervenção Federal no Estado do Rio de Janeiro, o que aumento exponencialmente as áreas onde eram as operações, com as ações conjuntas com outros órgãos do Governo. A figura abaixo, mostramos alguns locais onde os sensores foram disponibilizados:

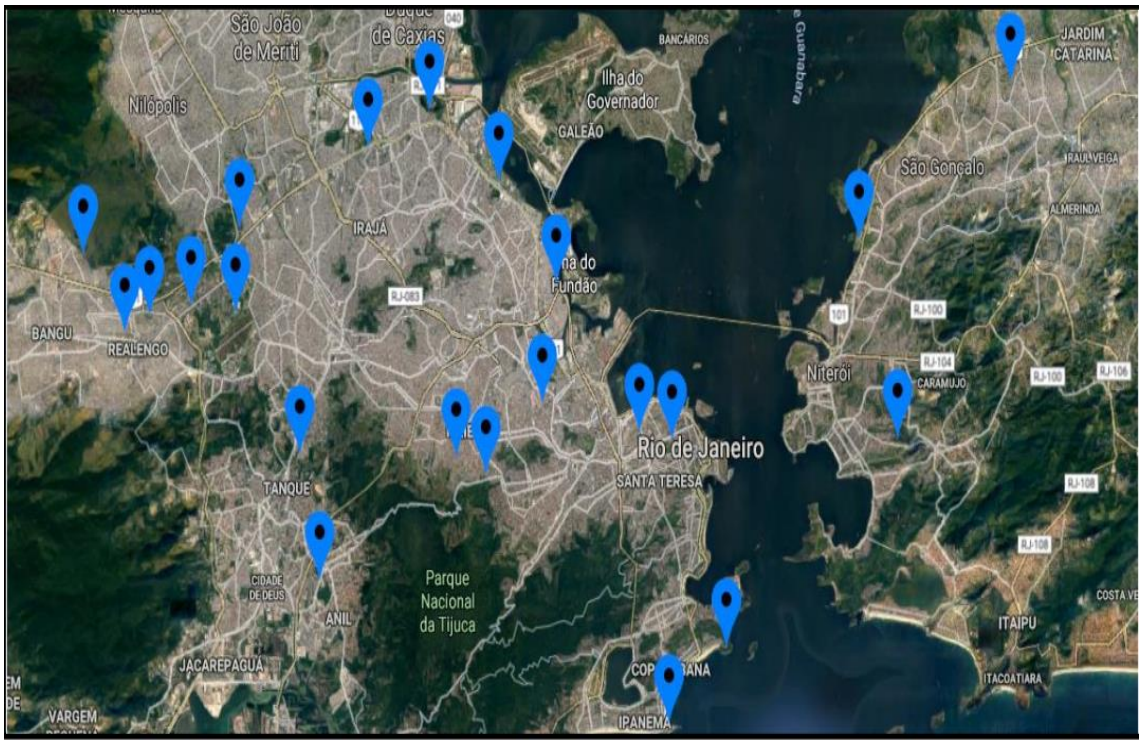

Figura 10: Desdobramento dos sensores MAGE durante a Intervenção Federal

Fonte: o autor, baseado em relatórios da operação

Por conta dessa amplitude no desdobramento dos meios de GE, começou-se a se pensar em utilizar os meios que o Exército Brasileiro dispõe, no caso sua

rede corporativa EBNet, para conectar os sensores ao COGE. Uma outra preocupação para se conectar a EBNet era através das outras redes das Forças Armadas (FA). Esse roteamento pode ser feito através da Rede Operacional de Defesa (ROD), que segundo o manual de Conceito Operacional do Sistema de Informação e de Apoio à Decisão para Comando e Controle (SIADC²) é:

> [...] a fornecedora dos enlaces de comunicações de dados militares operacionais. Está estruturada como uma *"Wide Area Network" (WAN)*, com conectividade segregada (restrita, segura e controlada) e diversificada, por meio do Sistema de Comunicações Militares por Satélite (SISCOMIS), das redes de dados das FA (RECIM, EBNET e INTRAER) e da Internet. (BRASIL,2019,p.18)

Isso foi devido ao fato de que algumas regiões onde ocorreram as operações eram em quartéis tanto da Marinha do Brasil, quanto da Força Aérea Brasileira. Para que isso acontecesse, foram feitos Reconhecimentos em todos esses locais, bem como contato com o 2º Centro de Telemática de Área, localizado no Comando Militar do Leste, o qual poderia fazer essa interface com os backhauls das outras FA.

Figura 11: Possível desdobramento dos sensores MAGE durante a Intervenção Federal
Fonte: o autor, baseado em relatórios da operação

3.3 Estado-Maior (EM)

Segundo o manual C101-5, o Estado-Maior é um conjunto simples e coeso, que deve trabalhar como uma equipe bem adestrada e cuja finalidade é assessorar o Cmt no cumprimento da missão. Ele possui duas estruturas, sendo uma delas o Estado-Maior Especial, como mostra a figura abaixo:

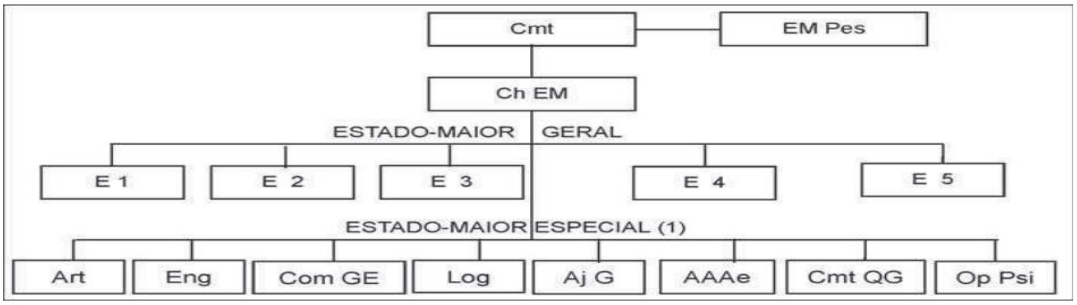

Figura 12: Estado-Maior
Fonte: BRASIL, 2003, p. 3-5

O Oficial de Ligação de GE está inserido nesse Estado-Maior Especial, na Seção COM GE. Sua função é coordenar as atividades relativas à sua seção com EM e com o Comando da Unidade de GE, de acordo com o manual GE na Força Terrestre (BRASIL,2019, p.7-6).

Segundo o manual Eletronic Warfare Techniques (ATP 3-12.3), do Exército dos Estados Unidos da América, existe um elemento do Batalhão de Guerra Eletrônica que irá fazer a Ligação com as Seções do Estado-Maior, coordenando e planejando suas operações.

Nos Grandes Eventos, bem como nas Op GLO, o O Lig GE teve um papel importante pois é o elo entre o COGE e o Estado-Maior, os quais são transmitidas e recebidas informações que serão válidas para o direcionamento do esforço dos Destacamentos de GE.

Este elemento do Estado-Maior Especial necessita conhecer sobre as funções de combate, principalmente, MANOBRA e INTELIGÊNCIA, pois irá suprir com informações de emprego de GE ao E3 de uma FTC ou ajudando o

E2 como confeccionar as perguntas para que se possa responder um PI, à luz da fonte de Sinais, de maneira mais completa possível.

Outro papel importante do O Lig GE é de explicar a atuação de GE para o Cmt FTC, bem como suas possibilidades e limitações, os quais poderão ser bastante úteis em um emprego coordenado de fogos cinéticos e não-cinéticos.

Todavia, ainda assim, nos relatórios, havia uma grande dificuldade em ter as informações de forma mais rápida e com mais riqueza de dados, os quais poderiam ser primordiais para o desenvolvimento das operações por parte de outras fontes de inteligência.

3.4 Centro de Operações de Guerra Eletrônica (COGE)

Segundo o manual GE nas Operações (EB70–MC–10.247), o COGE deve atender as características técnicas e táticas para a escolha do local de desdobramento. Nele, serão processados todos os dados obtidos de seus sensores para a produção de conhecimento. O local ao qual será desdobrado, segundo seu manual de emprego, pg.2-6, deve ter as seguintes características:

(1) oferecer possibilidade de ligações com os escalões superiores, apoiados; e elementos vizinhos;
(2) dispor de área compatível com a missão a ser desempenhada e com a situação tática;
(3) oferecer proteção contra os efeitos dos fogos do oponente;
(4) oferecer proteção contra o reconhecimento de combate e o reconhecimento aéreo;
(5) oferecer segurança às instalações; e
(6) dispor de acessibilidade compatível com as plataformas empregadas

O COGE também algumas atribuições, segundo o manual EB70–MC–10.247, na pg.2-9, que é o de:

a) receber as diretrizes, os planos e ordens do escalão apoiado;
b) ligar-se a outros órgãos de Guerra Eletrônica e Inteligência do Sinal, com a finalidade de obter informações e dados constantes do BD Sin e formar a base de dados de referência, para a atuação efetiva da GE na operação em curso, e remeter o conhecimento produzido àqueles órgãos;
c) realizar o planejamento e a condução das ações e atividades de GE executadas pelas frações da OM GE;
d) controlar a execução das ações ofensivas de GE das frações

> subordinadas e dos elementos recebidos em apoio;
> e) realizar a análise final, a partir dos relatórios oriundos dos COGE avançados;
> f) avaliar os resultados e produzir conhecimento, a partir dos sinais interceptados; e
> g) difundir os alarmes e conhecimentos produzidos ao escalão apoiado.

Com isso, podemos verificar que o COGE possui atribuições não somente de ligação com seus sensores, mas da análise que recebe dos mesmos. O COGE por muita das vezes, nas Op GLO e nos Grandes Eventos, foi desdobrado justaposto ao Posto de Comando (PC) da FTC ou do Comando Operativo. O que, por vezes, fez com que não houvesse tanta flexibilidade para o desdobramento de seus meios em áreas maiores, quiçá outras cidades/estados, por motivos doutrinários.

Em 2017, durante a Intervenção Federal no Estado do Rio de Janeiro, foi testado a utilização da rede corporativa do Exército, EBNet, para fazer o link entre os equipamentos e ter a condição de operá-los remotamente. Com o sucesso desses testes, foi utilizado o COGE do Destacamento de Guerra Eletrônica (Dst GE) numa Organização Militar e seus meios sendo acessados de forma remota, garantindo segurança para os integrantes do Dst GE, bem como facilidade de a Turma GE ter contato diretamente com os integrantes do COGE, agilizando a readequação dos meios de forma centralizada.

Nessa operação, também, foi montado um COGE paralelo ao da operação, no 1º BGE, o qual pode contribuir com o COGE Principal, devido à falta de efetivo e da missão ser bastante duradoura, como é mostrado na figura Nr13:

Figura13: COGE funcionando no 1º BGE

Fonte: o autor, que foi colocada nos relatórios da operação

Esse tipo de operação ficou muito semelhante ao que aos Centros Regionais de Monitoramento realizam, os quais sem premissa do tempo, ajudam a levantar o Banco de Dados da região, bem como podem operar de maneira remota, de acordo com o manual de campanha Guerra Eletrônica na Força Terrestre. A figura Nr 14 mostra como foi o acesso remoto a uma estação de GE:

Figura 14: Equipamento MAGE operado remotamente

Fonte: o autor, baseado em relatórios da operação

3.5 Central de Inteligência

Em Operações Militares de Não Guerra, a Inteligência, segundo o manual EB20-MC-10.207 Inteligência, pág 5-4:

> assume um papel de elevada relevância neste tipo de operação, uma vez que tem a capacidade de possibilitar uma adequada consciência situacional para o comandante operativo acerca do ambiente operacional e das ameaças existentes, produzindo conhecimentos de inteligência que também permitem uma antevisão das possíveis ações planejadas para serem desencadeadas pelas forças ou pelos agentes adversos, com potencial para influir nas operações militares da F Ter.

De acordo com o Manual EB20-MC-10.207 Inteligência, o ciclo de inteligência é o motor da função de combate inteligência, envolvendo direta ou indiretamente todos os integrantes da Força. Abaixo, segue as fases do ciclo:

Figura 15: Ciclo de Inteligência
Fonte: BRASIL,2015, p.4-1

O GE entraria na fase de obtenção, buscando dados não divulgados sobre alvos designados.

A estrutura e meios de uma Central de Inteligência, segundo o manual Batalhão de Inteligência Militar (EB70-MC-10.302), estão diretamente relacionados com a Operação a ser apoiada, com a complexidade dos conhecimentos necessários e com o volume de meios de obtenção de dados das diversas fontes empregadas. Durante as operações, a Central de Inteligência funciona da seguinte forma:

> a) Células de Análise (Cel Anl): compostas a partir da evolução das Turmas de Integração, de Anl Intlg, de CI e de Anl F Tecnl;

> b) Célula de Obtenção (Cel Obt): surge da evolução da Turma de Obtenção;
>
> c) Célula de Difusão de Informações: surge da Turma de Difusão de Informações. (BRASIL,2015, pág 3.7)

4. RESULTADOS E DISCUSSÃO

Espera-se que, com esse trabalho, seja possível verificar que o uso da EBNet possa ir além do uso administrativo no ambiente corporativo do EB, empregando esse recurso para apoio de operações de qualquer natureza, especialmente, nas de Guerra Eletrônica a fim de que sejam evidenciados os princípios de flexibilidade e modularidade.

Os Capitães, ALLAN e MICHELL, participaram de todos os Grandes Eventos e Missões de GLO no Brasil ao longo da última década. Suas experiências denotam que até a Intervenção Federal do Rio de Janeiro, os equipamentos de Guerra Eletrônica eram usados de forma remota através de links-rádio, formando uma rede que devia ser montada a cada operação. Durante a Intervenção, começaram a utilizar a EBNet, rede já previamente estabelecida, a qual foi de grande valia, pois aumentos a zona de atuação do Destacamento de Guerra Eletrônica.

Já os capitães THYAGO HENRIQUE e GABRIEL CASTRO, além de atuarem com os links-rádio e com o uso da EBNet, conseguiram utilizar sistemas VOIP para a comunicação com os postos rádios através de videoconferências.

Os capitães ALLAN, MICHELL e GABRIEL CASTRO participaram também da implementação do COGE dentro da célula de obtenção. Segundo eles, aumentou a consciência situacional sobre as operações em virtude dos dados obtidos pelas outras fontes circundarem de forma mais próxima e dinâmica pela fonte de sinais. Todo esse fluxo de mensagens se deu em virtude da EBNet, rede esta que fez aumentar a velocidade e segurança para que esse novo desdobramento fosse possível.

As respostas dos questionários realizados pelos antigos integrantes do 1º BGE mostram que houve uma evolução na forma de se organizar para a missões e de produzir conhecimento a partir da flexibilidade que o uso da rede corporativa do Exército consegue nos propor.

5. CONSIDERAÇÕES FINAIS

Inicialmente foi abordado sobre o conceito de operações, suas zonas de ação e rede de comunicações estabelecida durante Operações de Guerra e Não Guerra. O diferencial, inclusive abordado pelo manual Operation Urban FM 3-6, além do EB20-MF-10.103, manual Fundamento nas Operações, seria que a partir de um bom sistema de comunicações estabelecido, principalmente em ambientes urbanos, auxiliam o decisor a tomar suas linhas de ações por conta do fluxo rápido de informações que chegam até ele.

Camilo et al (2020) cita a diferença que numa área urbana, em detrimento de regiões rurais, seriam utilizados mais postos fixos, com até apropriação de meios urbanos para o fluxo de mensagens. É possível ver que além da utilização de rádios para o Comando e Controle de uma operação, o fluxo de dados, bem como a interligação dos meios de comunicações pode ser feita através de uma rede corporativa a qual, de forma segura e estável, irá nos propor benefícios que irão além da operação em si, mas com redução de custos, redução de pessoal e aumento da segurança para a nossa tropa.

Ao longo dos anos, no período de 2009 até 2021, houve inúmeras evoluções na GE, principalmente a que se remete a do Exército Brasileiro. Uma delas foram a compra de equipamentos com tecnologia de comunicações TCP/IP, as quais puderam interligar os diversos equipamentos através de uma rede. Com esse advento, alguns entusiastas de GE começaram a pensar na utilização da maior rede corporativa que o próprio Exército Brasileiro utiliza para quase todos os seus sistemas, no caso, a EBNet.

Não poderíamos deixar de citar tudo que a engloba, no caso o Sistema de Telemática do Exército (SisTEx), como todas as suas principais funções: conectividade, hospedagem, proteção cibernética e serviços de TI. A partir do momento que começaram a serem adquiridos equipamentos com protocolo de comunicações TCP/IP, e com todos os backbones da EBNet, podemos utilizar a rede em proveito das ações de GE, os quais precisam de uma rede de comunicações para o funcionamento completo de suas características, como por exemplo a Localização Eletrônica (LocElt). A utilização da tecnologia VOIP para comunicação e realização de videoconferências, através da EBNet, foi de suma

importância para o sucesso de inúmeras missões onde o único meio de contato seria através dessa rede, seja em quartéis, seja usando VPN, seja com o auxílio do SISCOMIS, link satelital, pela Rede Operacional de Defesa (ROD).

É possível estimar que tudo que trafegava estava, de certa forma, seguro, devido a proteção cibernética que é feita pelo SisTEx. Pudemos perceber que há uma preocupação contínua e são feitas campanhas para não deixarem de utilizar o antivírus nas máquinas que estão ligadas ao SisTEx, bem como os estabelecimento de vários níveis de segurança que auxiliam na proteção como Firewalls, autenticações, entre outros. Como poderemos ver a seguir o número de invasões diárias que sofre a rede EBNet:

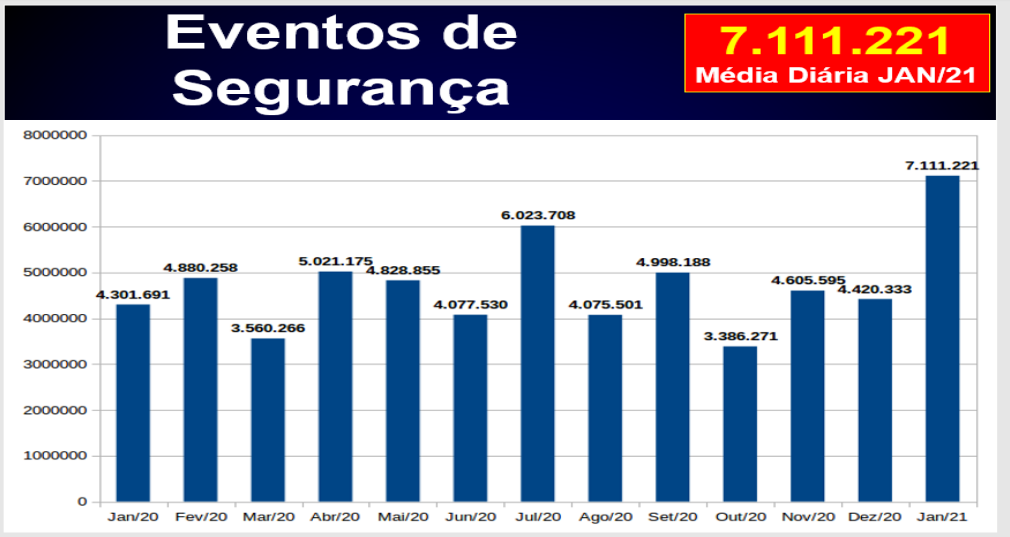

Figura 16: Número de tentativas de invasões diárias à EBNet
Fonte: Palestra ao PCI CCOM ESAO 2021 pelo CITEx

Com esse gráfico, podemos perceber o quão crítico é a importância de se manter os ambientes virtuais de forma segura, sendo um fator decisivo para o envio de mensagens e dados obtidos em prol das ações de GE. Os serviços de TI também são essenciais para as nossas operações a partir do momento em que são oferecidos internet, VOIP e videoconferência pelos meios do EB.

A partir disso, com estudos realizados nas Olímpiadas, bem como um apoio cerrado ao 2º CTA, começou a se fazer ingerências para que, na Intervenção Federal do Rio de Janeiro fossem operados, devido a área de atuação, os equipamentos de forma remota. Os testes foram feitos em bancada no 1º Batalhão de Guerra Eletrônica, sendo que todos, tanto os Operadores, bem

como os Analistas, foram treinados para que soubessem como iriam proceder no terreno, bem como transmitir suas demandas ao 2º CTA, como mostra a figura Nr 17:

Figura 17: Instrução para as operações
Fonte: o autor, baseado em relatórios da operação

No início da Intervenção Federal, foram formados Dst GE de 25 (vinte e cinco) militares, sendo 01(um) Ch Dst, 02 (dois) Anl e 22 (vinte e dois) Op. A partir do momento em que começaram a utilizar os equipamentos na rede da EBNet, conseguimos reduzir o efetivo das levas da missão, para somente 09 (nove) militares. Como o 1º BGE apoia todos os Comandos Militares de Área, apoiar de forma remota foi uma solução, durante as operações, que obteve sucesso e conseguiu reduzir, custos, a segurança ao nosso pessoal foi elevada, pois somente quem ficava no local era o equipamento, até por conta da frente sendo operado do COGE que ficava fixo no Batalhão Escola de Comunicações.

Essa mudança na forma de operar GE, prevista em manual, era somente feita a partir do momento em que se dava para realizá-la. Quando não se conseguia estabelecer uma conexão remota, as Turmas GE iam para o local da Operação, como no caso do Complexo do Alemão, onde não se havia qualquer ponto de EBNet próximo. Nesse caso, o O Lig GE, tinha sua relevância pois permanecia no Estado-Maior da Intervenção a fim de que fossem repassados os dados obtidos a todos de forma eficaz e rápida. Numa das operações foi colocado o COGE junto a célula de obtenção, a qual circundavam todas as informações de todas as fontes de inteligência. O simples fato de alocar essa estrutura nesse meio fez com que as Turmas GE fossem melhor direcionadas

em suas buscas, conseguindo mais informação de relevância para as operações.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL.Centro de Doutrina do Exército.EB70-MC-10.247, **Manual de Campanha A Guerra Eletrônica nas Operações**, Brasília-DF,1ª Ed, 2020;

BRASIL.Centro de Doutrina do Exército.EB70-MC-10.201, **Manual de Campanha A Guerra Eletrônica na Força Terrestre**. Brasília-DF, 1ª Ed, 2019;

BRASIL. Centro de Doutrina do Exército. C 101-5, **Estado-Maior e Ordens (1º Volume).** Brasília-DF, 2ª Ed., 2003;

BRASIL.Centro de Doutrina do Exército.EB20-MC-10.207, **Inteligência**. Brasília-DF, 1ª Ed, 2015;

BRASIL.Centro de Doutrina do Exército.EB20-MC-10.302, **Batalhão de Inteligência Militar**. Brasília-DF, 1ª Ed, 2018;

BRASIL.Centro de Doutrina do Exército.EB20-MC-10.223, **Manual de Campanha Operações**. Brasília-DF, 5ª Ed, 2017;

BRASIL.Centro de Doutrina do Exército.EB20-MF-10.103, **Manual de Fundamentos Operações**. Brasília-DF, 4ª Ed, 2014;

BRASIL.Centro de Doutrina do Exército.EB70-MC-10.201, **Manual de Campanha A Guerra Eletrônica na Força Terrestre**.Brasília-DF, 1ª Ed, 2019;

BRASIL.Ministério da Defesa.MD33-M-10, **Garantia da Lei e da Ordem.** Brasília-DF, 2ª Ed, 2014;

BRASIL.Ministério da Defesa.MD31-S-04, **Conceito Operacional do Sistema de Informação e de Apoio à Decisão para Comando e Controle (SIADC²).** Brasília-DF, 1ª Ed, 2019;

ESTADOS UNIDOS DA AMÉRICA. Headquarters, Department of Army USA. FM 2-0, **Intelligence.** Washington – DC, 2010;

ESTADOS UNIDOS DA AMÉRICA. Headquarters, Department of Army USA. ATP 3-12.3, **Eletronic Warfare Techniques.** Washington – DC, 2014.

ESTADOS UNIDOS DA AMÉRICA. Headquarters, Department of Army USA. FM 3-6. **Operation Urban.** Washington – DC, 2006;

CAMILO, Marcelo José; MOURA, David Fernandes Cruz; e SALLES, Ronaldo Moreira. **Redes de comunicações militares: desafios tecnológicos e propostas para atendimento dos requisitos operacionais do Exército Brasileiro**, Revista Militar de Ciência e Tecnologia, Vol XXXVII, 3º Trimestre de 2020;

APÊNDICE A – QUESTIONÁRIO

O presente questionário é parte integrante do trabalho de conclusão de curso em Ciências Militares do Cap Com Marcelo José Marquez de Campos, cujo tema é UTILIZAÇÃO DA INFRAESTRUTURA DE REDE DE COMUNICAÇÕES EXISTENTE NO EXÉRCITO BRASILEIRO PARA AS OPERAÇÕES DE GUERRA ELETRÔNICA. Pretende-se, através da dos dados obtidos, fornecer subsídios para a aceitação ou refutação da hipótese em estudo no trabalho. O senhor foi selecionado, dentro de um amplo universo, para responder as perguntas deste questionário. Solicito-vos a gentileza de respondê-lo o mais brevemente possível. A experiência profissional do senhor irá contribuir muito para a pesquisa, colaborando para os estudos referentes a utilização remota dos equipamentos GE/COGE através da EBNet. Este instrumento de pesquisa não precisa ser identificado. Suas respostas serão utilizadas para fins acadêmicos e terão seu sigilo preservado. Desde já agradeço a colaboração e coloco-me à disposição para esclarecimentos através dos seguintes contatos: Marcelo José Marquez de Campos *(Capitão de Comunicações – AMAN 2011) Celular: (61) 981443444 E-mail:marcelojmcampos@gmail.com*

1 – Por quantos anos o senhor serviu na 1ªCia GE/1º BGE?

2 - Quais operações de Guerra Eletrônica o senhor já participou?

3 – O senhor já havia participado de alguma atividade relacionada a Guerra Eletrônica de forma remota?

4 – O senhor, ao utilizar esse modo de operar, facilitou o comando e controle das ações de GE?

5 – O que isso melhorou como um contexto geral nas operações de GE?

6 – Como foi a inserção do COGE na Célula de Obtenção de Inteligência?