

A PROTEÇÃO DO FLUXO DA INFORMAÇÃO NO SISTEMA DE COMANDO E CONTROLE DA FORÇA TERRESTRE COMPONENTE

GUSTAVO OVÍDIO RIBEIRO DE CASTRO

Pós-graduado, Lato Sensu, em Gestão de Sistemas Táticos de Comando e Controle

RESUMO: A FORÇA TERRESTRE COMPONENTE É O COMANDO SINGULAR RESPONSÁVEL PELO PLANEJAMENTO E EXECUÇÃO DAS OPERAÇÕES TERRESTRES NO CONTEXTO DE UMA OPERAÇÃO CONJUNTA. NAS OPERAÇÕES, SERÁ INSTALADO UM SISTEMA DE COMANDO E CONTROLE QUE POSSUIRÁ UM CONJUNTO DE INSTALAÇÕES, EQUIPAMENTOS, SISTEMAS DE INFORMAÇÃO, COMUNICAÇÕES, DOCTRINA, PROCEDIMENTOS E PESSOAL ESSENCIAIS PARA O COMANDANTE PLANEJAR, DIRIGIR E CONTROLAR AS AÇÕES DE SUA ORGANIZAÇÃO PARA QUE SE ATINJA UMA DETERMINADA FINALIDADE. A OBTENÇÃO E A PROTEÇÃO DA INFORMAÇÃO CONSTITUEM-SE EM UM DOS PRINCIPAIS ELEMENTOS DO COMBATE MODERNO. A GUERRA DA INFORMAÇÃO É EXERCIDA DESDE OS TEMPOS DE PAZ E CONTRA DIFERENTES TIPOS DE AMEAÇA. NESSE CONTEXTO, O SISTEMA DE COMANDO E CONTROLE ESTÁ DIRETAMENTE RELACIONADO AO NOVO CENÁRIO DOS COMBATES MODERNOS QUE TEM POR OBJETIVO PRINCIPAL OBTER A SUPERIORIDADE DA INFORMAÇÃO POR MEIO DA GUERRA CENTRADA EM REDES. CRESCE, ASSIM, A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO, OU SEJA, TORNA-SE NECESSÁRIO ENTENDER QUAIS SÃO AS ATIVIDADES E AS TAREFAS NECESSÁRIAS PARA GARANTIR A PROTEÇÃO E A SEGURANÇA DAS INFORMAÇÕES GERADAS.

PALAVRAS-CHAVE: COMANDO E CONTROLE. GUERRA DA INFORMAÇÃO . SEGURANÇA DE INFORMAÇÃO.

1 INTRODUÇÃO

O presente artigo tratou sobre os aspectos relativos ao gerenciamento do fluxo da informação operativo no Sistema Comando e Controle da Força Terrestre quando do emprego do Exército Brasileiro nas operações.

A palavra informação conforme o Manual de Fundamentos Operações (BRASIL, 2014, p. 3-8) é o elemento fundamental da Era do Co-

nhecimento, e que, produzir, obter, utilizar e disseminar informações oportunas, objetivas e com credibilidade têm relação direta com a qualidade do processo decisório.

O Exército Brasileiro apresentou, em 2014, sua doutrina relativa as Operações de Informação por meio do Manual de Campanha EB-20-MC-10.213 Operações de Informação. Essas operações visam a evitar, impedir ou neutralizar os efeitos das ações adversas na Dimensão Informacional.

Desse conceito de Operações de Informações, abordagens relativas a Guerra da Informação podem ser observadas nas Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro:

XVI - Guerra da Informação: conjunto de ações destinadas a obter a superioridade das informações, afetando as redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos. (BRASIL, 2014, p. 12).

Com a crescente importância da informação precisamos entender como é o gerenciamento da informação nos sistemas de informação empregados no Exército Brasileiro. O Manual Comando e Controle (BRASIL, 2015, p 5-3) apresenta que com o aumento do volume e do fluxo de informações, o plano de gerenciamento de informação deve ser elemento primário do plano de operações.

Nessa linha de entendimento, referente a importância do gerenciamento da informação no Sistema de Comando e Controle, o Exército Brasileiro elaborou um manual para delegar as atribuições relativas a proteção. O Manual Proteção (BRASIL, 2015, p 3-2) cita que a célula de proteção coordena as atividades e sistemas



destinados a preservar a força por intermédio de uma sistemática de gerenciamento de risco, incluindo tarefas relacionadas as informações.

Portanto, para compreender o gerenciamento da informação, torna-se indispensável o entendimento sobre quais são as atividades e tarefas necessárias para garantir a proteção do fluxo da informação.

2 DESENVOLVIMENTO

2.1 METODOLOGIA

O artigo teve como objetivo geral compreender as atividades e as tarefas funcionais inerentes à proteção da informação no fluxo da informação no Sistema Militar de Comando e Controle da Força Terrestre Componente.

Como justificativa para o artigo pode-se verificar que na Doutrina de Operações Conjuntas do Ministério da Defesa consta uma estrutura de Comando e Controle com aspectos e procedimentos diferentes da existente no Exército Brasileiro. Tais procedimentos e estruturas podem ser adotados visando otimizar os procedimentos de proteção da informação nas operações.

Foi realizada uma pesquisa descritiva de cunho documental, sendo que a forma de abordagem utilizada foi a quantitativa. O delineamento de pesquisa contemplou as fases de coleta dos dados, comparação com a Doutrina Militar Terrestre, análise dos dados coletados e a discussão dos resultados.

Os assuntos do referencial teórico visam apresentar desde o entendimento macro das operações, envolvendo seu ambiente operacional, passando posteriormente pelo entendimento do Sistema de Comando e Controle e, por fim, compreendendo as atividades e tarefas dos elementos do Estado-Maior do Centro de Coordenação de Operações.

Por fim, os procedimentos adotados para o presente estudo foi a pesquisa doutrinária dos assuntos relativos a proteção da infor-

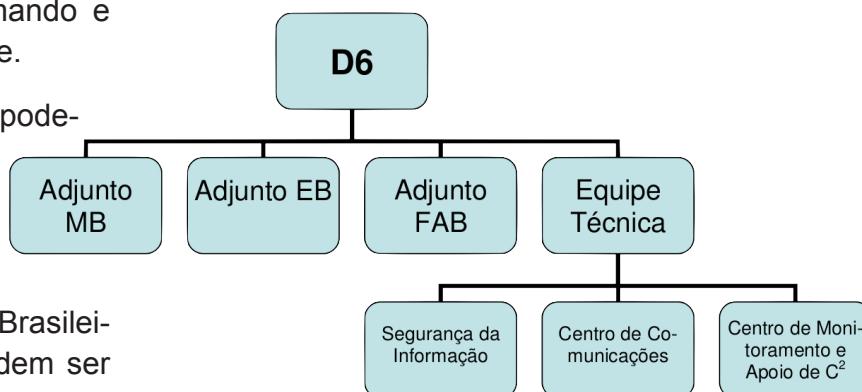
mação e as fontes de pesquisa foram manuais doutrinários do Ministério da Defesa e do Exército Brasileiro.

2.2 REFERENCIAL TEÓRICO

2.2.1 Comando e Controle na Doutrina de Operações Conjuntas

Na Doutrina de Operações Conjuntas do Ministério da Defesa pode-se verificar uma estrutura de Comando e Controle com aspectos e procedimentos que poderiam ser adotados pelo Exército Brasileiro, visando otimizar os procedimentos de proteção e segurança da informação nas operações.

FIGURA 1 - Estrutura da D6 no Estado-Maior Conjunto



Fonte: MD30-M-01, 2011, p 141

As atribuições inerentes a proteção da informação, que são de competência do setor de Segurança da Informação na Seção de Comando e Controle do Estado-Maior Conjunto, podem ser destacadas em: Instrução de Segurança da Informação, Plano de Adestramento de Segurança da Informação, assessorar no Plano de Segurança Orgânica e Gestão dos Sistemas de Informação.

Portanto, pode-se constatar que no Estado-Maior Conjunto já está normatizado os procedimentos relativos a proteção da informação.

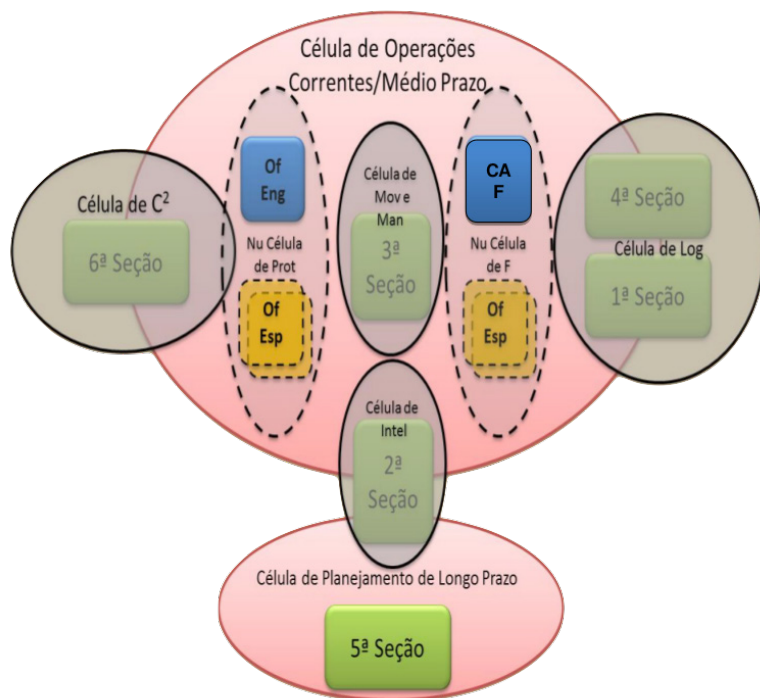
2.2.2 Comando e Controle na Força Terrestre Componente

O Estado-Maior da Força Terrestre Componente foi dividido em células funcionais e agora trabalha em um ambiente de interação e



integração das diversas especialidades, competências e capacitações existentes na Força Terrestre.

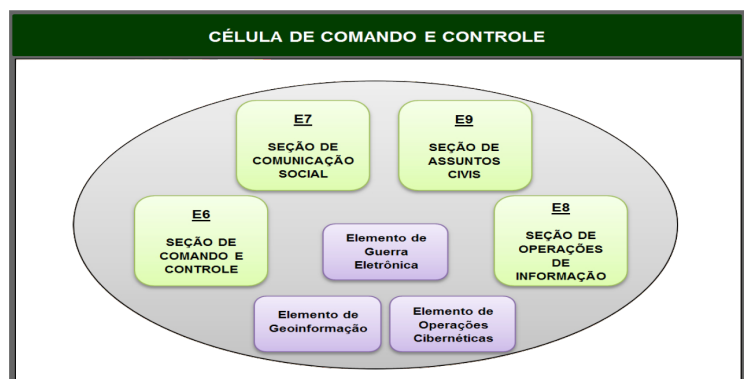
FIGURA 2 - Centro de Coordenação de Operações (CC Op) de um FTC



Fonte: BRASIL, 2014, p B-1

No esquema representado na figura acima, pode-se verificar uma área de interseção entre a Célula de Comando e Controle e a Célula de Proteção. Ou seja, existem atribuições e responsabilidades comuns no que se refere a proteção.

FIGURA 3 - Célular de Comando e Controle



Fonte: BRASIL, 2014, p 4-3

Na figura acima pode-se observar a existência de um Elemento de Operações Cibernéticas integrante da Célula de Comando e Controle do Centro de Coordenação de Operações da Força Terrestre Componente.

2.2.3 Atividades e Tarefas

2.2.3.1 Comando e Controle (C2)

Conforme Manual de Campanha EB-70-MC-10.341 Lista de Tarefas

Funcionais temos a seguinte atividade: realizar a gestão do conhecimento e da informação. Dentre outras, as tarefas podem ser verificadas a seguir:

- Estabelecer redes e sistemas de informações: compreende ampliar e defenderas redes de informação para garantir o fluxo das ordens e dos relatórios.
- Gerenciar informações e dados: compreende assegurar o acesso à informação com segurança e em níveis escalonáveis de usuários.
- Avaliar a informação coletada: compreende verificar a relevância da informação, realizando uma triagem inicial.
- Processar informações relevantes: compreende considerar imediatamente as informações críticas nas simulações e projeções para ajustar a operação constantemente. (BRASIL, 2016, p. 2-2)

2.2.3.2 Inteligência (Intlg)

Conforme Manual de Campanha EB-70-MC-10.341 Lista de Tarefas

Funcionais temos a atividade de apoio à obtenção da consciência situacional na qual apresenta, dentre outras, a tarefa a seguir:

Apoiar constantemente as atividades de ptç (C Intlg): esta tarefa tem como objetivos: impedir que ações hostis de qualquer natureza comprometam dados, informações, conhecimentos e sistemas a eles relacionados; impedir a realização de atividades de espionagem, sabotagem, propaganda hostil, terrorismo, desinformação; e induzir o centro de decisão do adversário a posicionar-se de forma equivocada. (BRASIL, 2016, p. 4-3)

2.2.3.3 Proteção (Ptç)

Conforme o EB70-MC-10.341 Lista de Tarefas Funcionais temos as atividades e tarefas, abaixo listadas, que tratam sobre informação:



QUADRO 1 - Atividades inerentes à função de combate proteção e suas tarefas

7.2 ADOPTAR MEDIDAS DE CONTRAINTELIGÊNCIA	
7.2.1 Tarefas:	a) Adotar medidas de segurança orgânica: visa a obter um grau de proteção ideal, por meio da adoção eficaz e consciente de um conjunto de medidas destinadas a prevenir e obstruir as ações de qualquer natureza que ameacem a salvaguarda de dados, conhecimentos e seus suportes do Sistema de Defesa. b) Adotar medidas de segurança ativa: destina-se a detectar, identificar, avaliar e neutralizar as ações da Inteligência adversa e outras ações de qualquer natureza, dirigidas contra os interesses da sociedade e do Estado.
7.7 REALIZAR MEDIDAS DE GUERRA CIBERNÉTICA	
7.7.1 Tarefas:	b) Adotar medidas de segurança de sistemas operacionais e serviços de rede em uso: consiste em estabelecer políticas de segurança da informação, acompanhadas de normas e procedimentos que possam ser implementados em quaisquer ambientes, independente do nível de conhecimento técnico dos usuários destes serviços. ... e) Estabelecer estrutura de segurança ofensiva: consiste em manter equipes multidisciplinares em condições de fazer frente a ameaças identificadas e com a finalidade de manter a iniciativa nas ações cibernéticas.

Fonte: BRASIL, 2016, p. 7-1 e 7-4 – adaptado pelo autor

Nesse contexto de proteção, o Manual de Campanha EB70-MC-10.232 Guerra Cibernética apresenta o seguinte conceito para Proteção Cibernética:

Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente. (BRASIL, 2017, p. 3-4)

2.2.4 Células Funcionais

2.2.4.1 Célula de Inteligência

As atribuições da Célula de Inteligência, com foco na segurança da informação, podem ser verificadas no Manual de Campanha EB-20-MC-10.202 FTC.

- d) produzir informações e conhecimentos, visando ao apoio à decisão do Cmt FTC e, quando pertinente, aos demais níveis decisórios;
- n) supervisionar a execução das medidas de contra inteligência;
- o) estabelecer, em coordenação com a Seção de Comando e Controle, a ar-

quitetura da rede de inteligência para troca de informações dentro do EM e com os elementos subordinados nos diferentes níveis;

t) fiscalizar e coordenar o acesso de militares ou representantes de governos ou de organizações estrangeiras a informações ou documentos sigilosos ou sensíveis; (BRASIL, 2014, p. 3-7 e 3-8)

2.2.4.2 Célula de Comando e Controle

O Manual de Campanha Força Terrestre Componente determina que o responsável pela estruturação do sistema de Comando e Controle da FTC, bem como por coordenar e disciplinar o seu funcionamento é o Chefe da Seção de Comando e Controle.

Dentre as atribuições listadas no manual acima referenciado, as que são diretamente relacionadas a gestão da informação podem ser verificadas na tabela.



QUADRO 2 - Atribuições inerentes ao Chefe da Célula de Comando e Controle

Atribuições	<p>c) planejar e coordenar a instalação, operação, manutenção e desmobilização de todos os sistemas de C2 da FTC, em coordenação com as demais seções do EM FTC;</p> <p>f) orientar o estabelecimento e o gerenciamento do banco de dados da FTC, contando com a contribuição das demais seções do EM para a sua atualização;</p> <p>h) planejar, coordenar e executar as medidas necessárias ao adestramento do pessoal necessário à operação do sistema de C2;</p> <p>i) coordenar com as seções de Operações e de Inteligência as atividades afetas à exploração do espectro eletromagnético e do ambiente cibernético, com vistas à obtenção de informações e à proteção de dados de interesse;</p> <p>j) estabelecer medidas de controle e segurança dos sistemas eletrônicos operados pelo comando da FTC;</p> <p>m) realizar a gestão das informações, em coordenação com outros membros do EM;</p>
-------------	--

Fonte: BRASIL, 2014, p. 3-10 e 3-11 – adaptado pelo autor

2.2.4.3 Célula de Proteção

O Manual de Campanha EB-20-MC-10.202 FTC determina que a Célula de Proteção coordena as atividades e sistemas destinados a preservar a força por intermédio de uma sistemática de gerenciamento de risco, a qual inclui tarefas relacionadas com a proteção do pessoal, dos meios físicos e das informações.

A célula é chefiada pelo Chefe da Seção Ptç e possui, dentre outras, as seguintes atribuições: analisar, planejar e coordenar as missões e atividades de proteção e propor diretrizes quanto ao emprego dos sistemas e execução das tarefas de proteção.

Da mesma forma, o EB20-MC-10.202 cita que a Célula de Proteção coordena com a Seção de Comando e Controle (6ª Seção) na Célula de Comando e Controle os aspectos relativos à tarefa de proteção da informação.

2.2.5 Oficiais / Elementos Especialistas

2.2.5.1 Elemento de Guerra Cibernética

Quanto aos aspectos de proteção cibernética, o Catálogo de Capacidades de Exército Brasileiro prevê que o Elemento de Guerra Cibernética deve conduzir ações para garantir o funcionamento dos nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e G Ciber para neutralizar ataques e exploração cibernética em nossos meios.

2.2.5.2 Oficial de Proteção das Operações

O EB20-MC-10.202 FTC apresenta o Oficial de Segurança das Operações como o responsável por desenvolver os procedimentos de segurança das operações. Além disso, suas atribuições incluem: revisar os documentos do EM FTC, os acessos aos sistemas de informação e as interações com a mídia.

O Manual de Campanha EB-20-MC-10.213 Operações de Informação cita, que o representante da Segurança das Operações, em coordenação com as outras Seções, é o responsável pela identificação das vulnerabilidades das nossas Capacidades Relacionadas à Informação e segurança das informações das nossas forças.

2.2.5.3 Oficial de Gestão do Conhecimento

O Oficial de Gestão do Conhecimento agrega ao EM FTC maior capacidade no que se refere à integração e ao gerenciamento de sistemas de informações. As suas principais atribuições são apresentadas no EB20-MC-10.202 FTC.

g) coordenar o apoio do E6 quanto à manutenção de redes, bancos de dados, armazenamento e assistência técnica; e (BRASIL, 2014, p. 3-18 e 3-19)

2.2.5.4 Oficial de Segurança da Informação (EM Cj)

Conforme a Doutrina de Operações



MD30-M-01, o Centro de Operações deve ter, em sua estrutura, um Oficial de Segurança da Informação, subordinado à D6 e trabalhando em estreita coordenação com a D2 do

Da mesma forma, a doutrina cita que cada F Cte deve indicar um Oficial de Segurança da Informação, responsável pelos seus respectivos sistemas.

QUADRO 3 - Atribuições inerentes ao Oficial de Segurança da Informação

Atribuições	<p>a) elaborar, divulgar e fiscalizar o cumprimento da Instrução de Segurança da Informação;</p> <p>b) elaborar e cumprir o Plano de Adestramento de Segurança da Informação do C Op;</p> <p>c) assessorar o Cmt Op nos assuntos de Segurança da Informação;</p> <p>d) propor, analisar e verificar se os requisitos de Segurança da Informação estão sendo cumpridos;</p> <p>e) identificar os integrantes do sistema que necessitem de proteção, de acordo com o grau de sigilo da informação por eles processada ou armazenada;</p> <p>f) assessorar a D2 na elaboração do Plano de Segurança Orgânico;</p> <p>g) reportar ao Cmt Op e aos demais Oficiais de Segurança da Informação do SISMC2, após uma avaliação preliminar, os incidentes de Segurança da Informação;</p> <p>h) controlar as autorizações para o acesso de usuários aos sistemas de informação do SISMC2;</p> <p>i) supervisionar a elaboração, o controle e a manutenção do histórico dos sistemas utilizados;</p> <p>j) analisar o impacto da descontinuidade dos serviços e suas consequências para o C Op, elaborando e testando um Plano de Contingência;</p> <p>k) exigir do pessoal externo ao C Op, autorizado a executar serviços no SISMC2, a assinatura de um Termo de Responsabilidade e o cumprimento das regras estabelecidas para guarda e proteção do sigilo das informações que possa ter acesso;</p> <p>l) empenhar-se para que os serviços (instalações, manutenções ou correções), sejam feitos sem afetar a Segurança da Informação; e</p> <p>m) fazer o possível para que todos os usuários estejam cientes das instruções em vigor para a Segurança da Informação, por meio da assinatura do Termo de Responsabilidade.</p>
-------------	---

Fonte: BRASIL, 2011, p. 121 – adaptado pelo autor

2.3 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

2.3.1 Na atividade de Comando e Controle

Tratando sobre como deve ser a atividade de proteção na gestão do Conhecimento e da Informação, pode-se constatar que as tarefas deverão primar pela manutenção fidedigna dos seguintes aspectos da informação: disponibilidade, integridade, confiabilidade, autenticidade e não repúdio.

Para estabelecer a Gestão da Informação nas redes e sistemas de Informações, constata-se a necessidade da elaboração de uma Política de Segurança da Informação, pela Célula de Comando e Controle, que contemple normas quanto à segurança física, lógica, de dados,

de usuários e de redes.

2.3.2 Na integração e interação entre as Células

Na revisão doutrinária, foi apresentado que o E6 identifica as vulnerabilidades e desenvolve procedimentos para proteger o Comando e Controle e a gestão de Sistemas de Informação e Comunicações. Da mesma forma, o E6 deverá colaborar com a confecção de planos relacionados à segurança das operações, particularmente vinculados à segurança das informações.

Com a criação da Seção de Segurança da Informação, subordinada a Seção de Comando e Controle, da Célula de Comando e Controle, seria possível realizar as atribuições pertinentes a proteção da informação haja vista a peculiaridade dos assuntos relativos a Segurança da Informação e Comunicações.



Dentre outras atribuições realizadas pela Seção de Segurança da Informação, podem ser destacadas: assessorar o Cmt Op nos assuntos de Segurança da Informação, assessorar a D2 na elaboração do Plano de Segurança Orgânica, controlar as autorizações para o acesso de usuários aos sistemas de informação do SISMC2 e empenhar-se para que os serviços (instalações, manutenções ou correções) sejam feitos sem afetar a Segurança da Informação.

Da mesma forma, em proveito da Função de Combate Proteção, a Seção de Segurança da Informação teria condições de realizar a tarefa de manter equipes multidisciplinares em condições de fazer frente a ameaças identificadas e com a finalidade de manter a iniciativa nas ações cibernéticas.

2.3.3 Nas responsabilidades funcionais

Primeiramente, uma tarefa ora atribuída ao Oficial de Gestão do Conhecimento é a de coordenar o apoio do E6 quanto à manutenção de redes, bancos de dados, armazenamento e assistência técnica. Tal tarefa de coordenação poderia ser realizada diretamente pelo Chefe da Célula de C2, pois é o responsável pela instalação do Sistema de C2, por intermédio da Seção de Comando e Controle.

Da mesma forma, não seria desejável que as responsabilidades inerentes a sistemas de informação fossem acumuladas pelo Oficial de Segurança das Operações, da Célula de Ptç. Tais motivos visam a segregação das informações que tramitam nos sistemas e o acúmulo demasiado de atribuições em um mesmo Oficial.

Quanto a documentação operacional empregada pela Força Terrestre Componente, poderia ser adotado o documento previsto para as Operações Conjuntas do Ministério da Defesa. O referido documento é o Apêndice Instrução de Segurança da Informação ao Anexo de C2 ao Plano Operacional, que seria confeccionado pelo Oficial de Segurança da Informação.

O Elemento de Operações Cibernéticas, integrante da Célula de Comando e Controle,

poderia ser o Oficial de Segurança da Informação e, conseqüentemente, o Chefe da Seção de Segurança da Informação.

Dentre as principais atribuições da seção podem ser destacadas: elaborar, divulgar e fiscalizar o cumprimento da Instrução de Segurança da Informação, controlar as autorizações para o acesso de usuários aos sistemas de informação do SISMC2 e fazer o possível para que todos os usuários estejam cientes das instruções para a Segurança da Informação.

3 CONCLUSÕES E RECOMENDAÇÕES

Neste artigo pode-se constatar um estudo sobre as atividades e tarefas necessárias para garantir a proteção do fluxo da informação no SISMC2 da FFTC para compreender os aspectos relativos ao gerenciamento da informação.

Tendo em vista a crescente importância da informação, foi necessário entender quais são as responsabilidades no gerenciamento da informação nos sistemas de informação empregados pelo Exército Brasileiro para verificar eventuais possibilidades de melhoria no emprego do referido Sistema de Comando e Controle.

O Sistema de C2 apresenta uma estrutura complexa, diversa e abrangente e, durante a pesquisa realizada, foi possível constatar que a Doutrina de Operações Conjuntas do Ministério da Defesa apresenta uma estrutura de Comando e Controle com aspectos e procedimentos diferentes dos preconizados pelo Exército Brasileiro

Para garantir um efetivo procedimento de controle sobre a segurança e a proteção do fluxo da informação no Sistema de C2, torna-se fundamental integrar e interagir as Células Funcionais de Inteligência, Comando e Controle e Proteção.

Primeiramente, verificou-se a viabilidade em adotar parcialmente a estrutura de C2 conforme a Doutrina de Operações Conjuntas no que se refere a criação da Seção de Segurança da Informação subordinada a Seção de C2, cuja



atribuição principal seria a de assessorar o Cmt Op nos assuntos de Segurança da Informação.

No segundo momento, teríamos a vinculação do cargo de Oficial de Segurança da Informação ao Elemento de Operações Cibernéticas, com a responsabilidade de elaborar, divulgar e fiscalizar o cumprimento da Instrução de Segurança da Informação por ocasião da exploração do Sistema de C2.

Por fim, verificou-se a possibilidade da adoção do Apêndice Instrução de Segurança da Informação ao Anexo de C2 ao Plano Operacional contendo os procedimentos e as atribuições necessárias às Seções do EM da FTC e as responsabilidades dos elementos integrantes do EM da FTC. Tal documento seria elaborado pelo Oficial de Segurança da Informação.

Portanto, o trabalho poderá servir para direcionar novas propostas de estudo sobre o assunto para que o resultado final seja a contribuição com o desenvolvimento doutrinário do Exército Brasileiro, visando ampliar os aspectos de proteção do fluxo da informação no Sistema de C2 da Força Terrestre.

THE PROTECTION OF THE INFORMATION FLOW IN THE COMMAND AND CONTROL SYSTEM OF THE GROUND FORCE COMPONENT

ABSTRACT: THE COMPONENT GROUND FORCE IS THE ONLY COMMAND RESPONSIBLE FOR PLANNING AND EXECUTING GROUND OPERATIONS IN THE CONTEXT OF A JOINT OPERATION. IN OPERATIONS A COMMAND AND CONTROL SYSTEM WILL BE INSTALLED WHICH WILL HAVE A SET OF ESSENTIAL FACILITIES, EQUIPMENT, INFORMATION SYSTEMS, COMMUNICATIONS, DOCTRINES, PROCEDURES AND PERSONNEL FOR THE COMMANDER TO PLAN AND CONTROL THE ACTIONS OF HIS ORGANIZATION TO ACHIEVE A PURPOSE. OBTAINING AND PROTECTING INFORMATION IS ONE OF THE MAIN ELEMENTS OF MODERN COMBAT. INFORMATION WARFARE HAS BEEN CARRIED OUT SINCE TIMES OF PEACE AND AGAINST DIFFERENT TYPES OF THREATS. IN THIS CONTEXT, THE COMMAND AND CONTROL SYSTEM IS DIRECTLY RELATED TO THE NEW SCENARIO OF MODERN COMBATS WHOSE MAIN OBJECTIVE IS TO OBTAIN INFORMATION SUPERIORITY THROUGH NETWORK

WARFARE. THUS, THE IMPORTANCE OF INFORMATION SECURITY IS INCREASED, THAT IS, IT BECOMES NECESSARY TO UNDERSTAND WHAT ACTIVITIES AND TASKS ARE NECESSARY TO ENSURE THE PROTECTION AND SECURITY OF THE INFORMATION GENERATED.

KEYWORDS: COMMAND AND CONTROL, INFORMATION WARFARE AND INFORMATION SECURITY.

REFERÊNCIAS

BRASIL. Estado-Maior do Exército Brasileiro. Manual de Campanha E20-MC-10.202 Força Terrestre Componente. 1. ed. Brasília, 2014.

_____. _____. Manual de Campanha EB20-MC-10.205 Comando e Controle. 1. ed. Brasília, 2015.

_____. _____. Manual de Campanha EB20-MC-10.208 Proteção. 1. ed. Brasília, 2015.

_____. _____. Manual de Campanha EB20-MC-10.213 Operações de Informação. 1. ed. Brasília, 2014.

_____. _____. Manual de Campanha EB70-MC-10.232 Guerra Cibernética. 1. ed. Brasília, 2017.

_____. _____. Manual de Campanha EB70-MC-10.341 Lista de Tarefas Funcionais. 1. ed. Brasília, 2016.

_____. _____. Manual de Fundamentos EB20-MF-10.103 Operações. 4. ed. Brasília, 2014.

_____. _____. Portaria nº 803-Cmt Ex, de 30 de julho de 2014: Aprova as Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro - EB10-IG-01.014. Brasília, 2014.

_____. Ministério da Defesa. MD30-M-01: Doutrina de Operações Conjuntas – 3º Volume. 1. Ed. Brasília, 2011.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras - AMAN (2006), pós graduado em Guerra Eletrônica pelo Centro de Instrução de Guerra Eletrônica - CIGE (2011), em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais - EsAO (2015) e em



Gestão de Sistemas Táticos de Comando e Controle pela Escola de Comunicações - EsCom (2017) e pode ser contactado pelo e-mail ovidio.gustavo@eb.mil.br.

