MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
GAB CMT EX – CIE
ESCOLA DE INTELIGÊNCIA MILITAR DO EXÉRCITO

CURSO AVANÇADO DE INTELIGÊNCIA PARA OFICIAIS

TRABALHO DE CONCLUSÃO DE CURSO

A IMPORTÂNCIA DO ESTUDO DE SITUAÇÃO DE CONTRAINTELIGÊNCIA PARA O GERENCIAMENTO DOS RISCOS OPERACIONAIS LEVANTADOS DURANTE O PROCESSO DE PLANEJAMENTO E CONDUÇÃO DAS OPERAÇÕES MILITARES EM SITUAÇÃO DE GUERRA

Brasília
2023

Maj JOSÉ REINALDO **SANTOS JÚNIOR**

A IMPORTÂNCIA DO ESTUDO DE SITUAÇÃO DE CONTRAINTELIGÊNCIA PARA O GERENCIAMENTO DOS RISCOS OPERACIONAIS LEVANTADOS DURANTE O PROCESSO DE PLANEJAMENTO E CONDUÇÃO DAS OPERAÇÕES MILITARES EM SITUAÇÃO DE GUERRA

Trabalho de Conclusão de Curso apresentado à Escola de Inteligência Militar do Exército, como requisito para a obtenção do Grau de Pós-graduação *Lato Sensu* de **Especialização em Análise de Inteligência.**

Orientador: Ten Cel DANIEL PASCHOAL **ZANINI**

Brasília
2023

CATALOGRAÇÃO NA FONTE
BIBLIOTECA CEL FORRER GARCIA

S237i Santos Júnior, José Reinaldo

A importância do Estudo de Situação de Contrainteligência para o gerenciamento dos riscos operacionais levantados durante o processo de planejamento e condução das Operações Militares em situação de guerra / José Reinaldo Santos Júnior – 2023.
33 f.

Orientador: Daniel Paschoal Zanini
Trabalho de Conclusão de Curso (Especialização em Análise de Inteligência) - Escola de Inteligência Militar do Exército (EsIMEx), Brasília – DF, 2023.

1. Contrainteligência 2. Exame de Situação de Contrainteligência 3. Risco 4. Gerenciamento de Risco 5. Operação Militar 6. Ameaças. I. Título.

Maj JOSÉ REINALDO **SANTOS JÚNIOR**

A IMPORTÂNCIA DO ESTUDO DE SITUAÇÃO DE CONTRAINTELIGÊNCIA PARA O GERENCIAMENTO DOS RISCOS OPERACIONAIS LEVANTADOS DURANTE O PROCESSO DE PLANEJAMENTO E CONDUÇÃO DAS OPERAÇÕES MILITARES EM SITUAÇÃO DE GUERRA

Trabalho de Conclusão de Curso apresentado à Escola de Inteligência Militar do Exército, como requisito para a obtenção do Grau de Pós-graduação *Lato Sensu* de **Especialização em Análise de Inteligência.**

Aprovado em 19 de junho de 2023.

COMISSÃO DE AVALIAÇÃO:

_____
DANIEL PASCHOAL **ZANINI** – TC **-** Presidente
Escola de Inteligência Militar do Exército

_____
CARLOS ROGÉRIO DE FREITAS **PACCIULLI -** TC - Membro
Escola de Inteligência Militar do Exército

RESUMO

A complexidade das operações militares requer soluções cada vez mais eficazes, no intuito de promover o máximo aproveitamento das capacidades de todas as células de planejamento do Estado-Maior em prol do melhor custo-benefício para o cumprimento da missão. Nesse sentido, o presente estudo pretende apresentar a contribuição do exame de situação de contrainteligência e de seus produtos, como ferramenta para o mapeamento das ameaças componentes da matriz de gerenciamento de riscos de uma operação militar de guerra, a fim de entender como se realiza a integração entre os dois processos. Por meio de uma análise de livros, manuais doutrinários e diversos artigos científicos e revistas relacionadas ao tema, foram analisadas as etapas componentes do exame de situação de contrainteligência e do processo de gerenciamento de riscos operacionais, com enfoque voltado para uma situação de guerra, e ao final, foram apresentados aspectos atinentes aos dois processos que com uma correta e oportuna integração tem o potencial de reduzir os riscos de uma Operação Militar.

Palavras-chave: Contrainteligência. Exame de Situação de Contrainteligência. Risco. Gerenciamento de Risco. Operação Militar. Ameaças.

RESUMEN

La complejidad de las operaciones militares requiere de soluciones cada vez más efectivas, a fin de promover el máximo aprovechamiento de las capacidades de todas las células de planificación del Estado Mayor en favor del mejor costo-beneficio para el cumplimiento de la misión. En ese sentido, el presente estudio pretende presentar el aporte del diagnóstico situacional de contrainteligencia y sus productos, como herramienta de mapeo de las amenazas que componen la matriz de gestión de riesgos de una operación militar de guerra, con el fin de comprender cómo se produce la integración entre los dos procesos A través del análisis de libros, manuales doctrinales y diversos artículos y revistas científicas relacionados con el tema, se analizaron las etapas que componen el examen de situación de contrainteligencia y el proceso de gestión del riesgo operacional, con enfoque en una situación de guerra, y al final, aspectos relacionados con los dos procesos que, con una correcta y oportuna integración, tienen el potencial de reducir los riesgos de una Operación Militar.

Palabras Clave: Contrainteligencia. Examen de Situación de Contrainteligencia. Riesgo. Gestión de riesgos. Operación militar. Amenazas.

SUMÁRIO

1 INTRODUÇÃO

A segurança é o segundo nível da hierarquia das necessidades constante da Pirâmide de Maslow, se posicionando logo após as necessidades fisiológicas como fome, sede e a respiração. Nas variadas atividades pessoais e profissionais, o ser humano busca adotar medidas que reduzam eventuais riscos, aumentando a sensação de segurança.

Modernamente, o mundo corporativo passou a estudar processos metodológicos de gerenciamento e análise de riscos, com o objetivo de reduzir vulnerabilidades, impedir que ameaças explorem vulnerabilidades ainda existentes, limitar impactos de eventos adversos e minimizar riscos.

Seguindo essa linha, as Instituições Públicas e Privadas enfrentam questões relativas a como proteger seus ativos das ameaças presentes no cotidiano. No Exército não poderia ser diferente. A proteção dos ativos da Força Terrestre é uma preocupação constante e não há como se obter sucesso sem um correto mapeamento das ameaças existentes.

Em se tratando de uma situação de guerra, o gerenciamento dos riscos oriundos da atuação das ameaças em nossas vulnerabilidades pode determinar o sucesso ou o fracasso das Operações Militares.

O Manual EB70-MC-10.223, Operações, traz o conceito de Operação Militar como sendo:

> O conjunto de ações realizadas com forças e meios militares. São coordenadas no espaço, tempo e finalidade, devendo ser estabelecida uma diretriz, plano ou ordem para cumprir a missão, tarefa, atividade ou atribuição (Brasil, 2017a, p. 2-1).

Gerenciar riscos é fator decisivo para o sucesso de uma Operação Militar. A Política de Gestão de Riscos do Exército Brasileiro define risco como “uma possibilidade de ocorrência de um evento que trará um impacto no cumprimento dos objetivos que a instituição estabeleceu” (Brasil, 2018).

A atividade de gerenciamento de risco deve estar inserida no planejamento e na execução das operações. Os comandantes, de maneira geral, deverão estar aptos a trabalhar com essa ferramenta. Segundo Gallagher (2014), a capacidade de gerenciar riscos de modo efetivo, deve ser uma das características mais importantes de um comandante.

Para o correto e eficiente gerenciamento dos riscos, faz-se necessária a utilização de todas as ferramentas capazes de identificar as ameaças. Por isso, os serviços de Inteligência têm sido elevados a um papel fundamental na busca por prevenção das vulnerabilidades apresentadas no campo de batalha (Brasil, 2020).

A Inteligência se ocupa de temas do âmbito externo e interno do país. No âmbito externo, tem como missão obter e analisar dados que ofereçam suporte aos objetivos nacionais, tanto na defesa contra as ameaças existentes quanto na identificação de oportunidades.

A atividade de Inteligência é fundamental e indispensável à segurança dos Estados, da sociedade e das instituições nacionais. Sua atuação assegura ao poder decisório o conhecimento antecipado e confiável de assuntos relacionados aos interesses nacionais (ABIN, 2019).

Hoje, sem o uso da inteligência no combate moderno, as dificuldades de prevenção e neutralização das ameaças reduzem bastante, tendo em vista o dinamismo e as capacidades tecnológicas desenvolvidas pelos mais variados oponentes (Brasil, 2020b).

O presente trabalho tem como objetivo geral, avaliar a contribuição do exame de situação de contrainteligência e de seus produtos, para o gerenciamento de riscos de uma operação militar de guerra, a fim de estudar como se realiza a integração entre os dois processos.

Deste modo, este estudo está estruturado em três Seções, de modo a alcançar os objetivos específicos propostos. A primeira se propõe a realizar uma análise do exame de situação de contrainteligência, com o estudo das etapas componentes do processo. O segundo capítulo visa analisar o processo de gerenciamento de risco operacional, detalhando todas as suas fases. Por fim, o terceiro capítulo tem por objetivo apresentar as contribuições do estudo de situação de contrainteligência para o processo de gerenciamento de riscos operacionais em situação de guerra.

2 O EXAME DE SITUAÇÃO DE CONTRAINTELIGÊNCIA

2.1 CONSIDERAÇÕES INICIAIS

A Política Nacional de Inteligência, documento de mais alto nível que rege a atividade de inteligência no nosso país, adota o conceito de contrainteligência como sendo:

> A atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado (Brasil, 2016).

O Manual EB70-MF-10.107, Inteligência Militar Terrestre, se refere ao ramo contrainteligência da seguinte forma:

> Por sua natureza, as atividades e tarefas ligadas à C Intlg estão afetas à Função de Combate Proteção. Elas permitem identificar, prevenir e mitigar ameaças às forças e aos meios vitais para as operações, de modo a preservar o poder de combate e a liberdade de ação (Brasil, 2015, p.4-2).

Portanto, atribui-se à atividade de contrainteligência a função de segurança e proteção dos ativos, constituindo-se no ramo da Atividade de Inteligência Militar que tem como missão salvaguardar os recursos humanos, as informações, o material e as áreas e instalações que o Exército Brasileiro tenha interesse de preservar (Brasil, 2016).

“As atividades e tarefas concernentes a esse ramo da Inteligência Militar são desenvolvidas de forma constante e ininterrupta, buscando-se a antecipação diante das potenciais ações hostis contra a Força” (Brasil, 2019, p.1-2).

Importante salientar que as atividades de contrainteligência não se limitam aos tempos de paz, pois devem ser executadas desde a situação de normalidade. De acordo com o Manual EB70-MC-10.307, Planejamento e Emprego da Inteligência Militar, “em operações, a atuação da Contrainteligência alcança seu nível mais elevado de desenvolvimento” (Brasil, 2016, p.4-2).

Em situação de guerra, a análise da ameaça inicia-se na segunda fase do Processo de Planejamento e Condução das Operações Terrestres, denominada situação e sua compreensão.

O Manual EB70-MC-10.220, Contrainteligência, define ameaça como:

> A conjunção de ator, motivação e capacidade de realizar ação hostil, real ou potencial, com possibilidade de, por intermédio da exploração de deficiências, comprometer as informações, afetar o material, o pessoal e

> seus valores, bem como as áreas e instalações, podendo causar danos ao Exército (Brasil, 2019, p.2-1).

Nas Operações, o foco da atividade de contrainteligência se volta para as possibilidades das forças inimigas obterem conhecimentos, dados, informações sensíveis ou críticas, além das atividades de espionagem, sabotagem, terrorismo, propaganda adversa e desinformação.

A contrainteligência exerce papel fundamental tanto na função de combate inteligência, como também na função de combate proteção. Na função de combate inteligência, cumpre a tarefa de assegurar a compreensão sobre as ameaças atuais e potenciais. Já na função de combate proteção, busca levantar as potenciais vulnerabilidades de nossas tropas.

O Manual EB20-MF-10.207, Inteligência, estabelece a seguinte ligação entre as funções de combate proteção e inteligência:

> A primeira constitui um conjunto de tarefas e sistemas que se destinam a preservar a força, a fim de possibilitar ao comandante o máximo poder de combate disponível para o cumprimento da missão e a segunda, em seu ramo de contrainteligência, tem por objetivo proteger os sistemas operativos e as estruturas de inteligência das nossas tropas (Brasil, 2015, 2-7).

Para cumprir as tarefas acima descritas, o planejamento de contrainteligência obedece a metodologias que visam sistematizar e dar maior eficácia e eficiência ao trabalho de Estado-Maior, quer seja em situação de guerra ou de paz.

Para a situação de paz, o Manual EB- 70-MC-10.220, Contrainteligência, apresenta uma concepção de Planejamento de Contrainteligência e divide seu desenvolvimento em duas fases: o Exame de Situação e o Processo de Desenvolvimento da Contrainteligência (PDCI). Para a situação de guerra, foco deste trabalho, o mesmo manual aduz que: “no que couber, o planejamento de Contrainteligência relacionado às operações deve seguir o prescrito no Manual de Campanha Planejamento e Emprego da Inteligência Militar” (Brasil, 2019c, p. 5-1).

Para isso, o Manual EB- 70-MC-10.307, Planejamento e Emprego de Inteligência Militar também apresenta uma metodologia para a realização do exame de situação de contrainteligência, voltado para uma situação de guerra, que passaremos a analisar a seguir e que servirá de base para a confecção do Plano de Contrainteligência da Operação.

Segundo Brasil (2016), este exame é uma avaliação das possibilidades da Inteligência inimiga, a fim de determinar a probabilidade relativa e a potencialidade dessas possibilidades e os consequentes efeitos sobre nossas linhas de ação.

A base desse estudo é centrada na Ordem de Batalha das Unidades Inimigas, bem como nos Órgãos que executam suas capacidades relacionadas à informação (inteligência, comunicação social e operações psicológicas).

2.2 ETAPAS DO PROCESSO

O exame de situação de contrainteligência é dividido em 04 (quatro) etapas, conforme se segue:

A primeira etapa é a análise da missão. Da mesma forma que no exame de situação preconizado no Processo de Planejamento e Condução das Operações Terrestres, nesta etapa inclui-se o entendimento da relação do escalão considerado com a missão dos escalões superiores e outras Forças envolvidas na Operação, contudo, sob a ótica da contrainteligência:

> A finalidade da análise da missão é fazer com que o comandante adquira uma ideia clara e completa das principais ameaças e vulnerabilidades envolvidas na operação. Com isso, poderá identificar os principais ativos a serem protegidos, de acordo com os grupos de medidas da segurança orgânica e ativa (Brasil, 2016, 4-2).

A Contrainteligência deve pensar além de uma ação hostil óbvia, pois contra ela, normalmente, haverá uma proteção adequada. A Contrainteligência busca, principalmente, o que está além da linha do trivial.

Na segunda etapa, são levantadas as características da Área de Operações, abrangendo a Zona de Ação e a Área de Interesse. Nesse momento são analisados os aspectos relativos às Forças Amigas, Inimigo, Terreno, Condições Meteorológicas e Considerações Civis.

No que diz respeito às Forças Amigas, o exame de situação de contrainteligência dá ênfase nas nossas vulnerabilidades ante a capacidade inimiga de busca de conhecimento e/ou de realização de ações hostis (Brasil, 2019). São levantadas as vulnerabilidades referentes à segurança ativa e segurança orgânica, esta última dentro dos grupos de medidas. Além disso, nesta etapa também são levantados os principais ativos e meios críticos a serem protegidos durante todas as fases da Operação.

Prosseguindo na segunda etapa, inicia-se o estudo do inimigo com os dados gerais disponíveis. Cabe ressaltar que os aspectos relacionados ao Inimigo, nesse

momento, ainda são analisados de forma superficial, haja vista que a terceira e quarta etapa realizam esse estudo de uma forma mais completa e aprofundada.

O terreno é analisado com o enfoque voltado para os aspectos que podem ser explorados pelas ameaças para causar danos às nossas forças, tais como: condições de aproveitamento de recursos locais por parte do inimigo, presença de obstáculos que possam canalizar ou dificultar o movimento de nossas tropas, permitindo ações hostis do inimigo, condições gerais para o deslocamento de Tr a pé e embarcadas, vias de acesso, disponibilidade de cobertas e abrigos, dentre outros aspectos que podem vir a se tornar vulnerabilidades a serem exploradas pelo oponente.

A análise das condições meteorológicas e das considerações civis também seguem a mesma lógica até aqui apresentada, ou seja, o foco se dá no levantamento de nossas vulnerabilidades e nas capacidades inimigas de aproveitar essas vulnerabilidades, de modo a permitir o planejamento de medidas para mitigar riscos.

No que tange às condições meteorológicas são analisados aspectos referentes à temperatura, precipitações e luminosidade que podem interferir nas Operações ou serem aproveitados pelo inimigo contra nossas Forças.

No que diz respeito às considerações civis, a análise se debruça sobre aspectos que podem comprometer a segurança das operações, baseado nos dados levantados e nas informações obtidas pelo escalão superior.

Na terceira etapa, denominada situação das forças inimigas, faz-se uma análise mais aprofundada sobre as atividades inimigas, particularmente, dos seus Órgãos de Inteligência e de Unidades com capacidade de realizar ações de sabotagem, terrorismo, espionagem, operações psicológicas e desinformação. (Brasil, 2019).

> São considerados, quando possível, dados e/ou conhecimentos relativos à doutrina, organização, instrução, desdobramento, material, composição, efetivos, características, técnicas, possibilidades e vulnerabilidades dos meios executantes daquelas atividades e ações (Brasil, 2016, p.4-4).

Essencial que sejam identificadas todas as forças adversas que atuam na Área de Operações, incluindo, organizações criminosas, grupos hostis e organizações terroristas. Cabe ressaltar que é nessa etapa que são levantados todos os conhecimentos que o inimigo porventura possua sobre nossa inteligência e contrainteligência.

Na quarta e última etapa do exame de situação de contrainteligência são estudadas as capacidades das Forças Inimigas.

> É uma avaliação das possibilidades das diversas fontes de Inteligência e Contrainteligência inimiga (humanas, imagens, sinais e cibernética), bem como de suas Unidades e Órgãos com capacidade de realizar sabotagem, terrorismo, espionagem, operações psicológicas, propaganda e desinformação, a fim de determinar a probabilidade relativa e a potencialidade dessas possibilidades e os consequentes efeitos sobre nossas linhas de ação (Brasil, 2016, 4-5).

O estudo dessas capacidades permeia todas as fases do planejamento da Operação, analisando a probabilidade de interferência nos principais ativos levantados na primeira etapa do exame de situação de contrainteligência.

O capítulo IV, do Manual EB- 70-MC-10.307, que trata sobre o exame de situação de contrainteligência, descreve somente as quatro etapas mencionadas acima. Contudo, da análise do “Anexo l” e “Anexo J”, do mesmo documento doutrinário, verifica-se a previsão do gerenciamento dos riscos identificados, com base no levantamento das nossas vulnerabilidades e na capacidade do inimigo, seguindo o modelo preconizado no Manual de Contrainteligência.

De acordo com Brasil (2019), o gerenciamento dos riscos no processo de exame de situação de contrainteligência obedece a cinco fases distintas, quais sejam: identificação dos riscos, análise dos riscos, avaliação dos riscos, linhas de ação e decisão.

Na primeira fase são identificados todos os riscos, internos e externos, levando-se em consideração os principais ativos existentes. Nesse momento, recomenda-se a utilização de lista de verificação (*checklist*) ou a técnica de *Brainstorming* para geração de ideias. Os riscos levantados são tabulados em formato de tabela, na qual são atribuídos códigos dos riscos, os possíveis atores, ações, motivações e deficiências.

Após identificados, em uma segunda fase, os riscos são analisados de forma qualitativa quanto à probabilidade de ocorrência e impacto que podem causar. “Para isso, são utilizados critérios preestabelecidos, com uma escala para determinar o valor de cada risco” (Brasil, 2019, p.5-9).

Em uma terceira fase, esses riscos são avaliados, estabelecendo os níveis de risco, que podem ser: baixo, médio, alto e extremo.

O valor do risco é estabelecido mediante o emprego da Matriz de Exposição a Riscos. Para tanto, multiplica-se a probabilidade pelo impacto para se obter o nível de risco correspondente.

> Os níveis de risco são estabelecidos mediante a combinação das dimensões probabilidade x impacto, da seguinte forma:
> a) Área Vermelha - riscos extremos, que exigem a implementação imediata das ações de proteção e prevenção. São eventos que devem ser monitorados prioritariamente;
> b) Área Laranja - riscos altos, que devem gerar respostas rápidas, planejadas e testadas em planos de segurança. São eventos que devem ser constantemente monitorados;
> c) Área Amarela - riscos médios, que devem ser monitorados de forma rotineira e sistemática; e
> d) Área Verde - riscos baixos, que representam pequenos danos. Esses riscos podem ser somente gerenciados e administrados.

Figura 1 - Matriz de Exposição a Riscos

Fonte: Manual EB- 70-MC-10.220 (Brasil, 2019).

Em seguida, na quarta fase, são elaboradas as linhas de ação para o tratamento dos riscos. O tratamento decorre das seguintes possibilidades: aceitar, compartilhar, evitar ou mitigar.

Na possibilidade de aceitar o risco, nenhuma medida é adotada para reduzir a probabilidade ou o grau de impacto do risco. No grau compartilhar ocorre a redução da probabilidade ou do impacto do risco pela transferência ou pelo compartilhamento de uma porção do risco. Já no nível evitar, há um abandono das atividades que geram riscos. Já no grau mitigar, ocorre a adoção de medidas visando a reduzir a probabilidade, o impacto ou ambos.

Por fim, após a elaboração de no mínimo 02 (duas) linhas de ação para cada risco e atendendo o princípio da oportunidade, o comandante toma a decisão de quais linhas de ação adotar.

Desta forma, conclui-se parcialmente que, a despeito do processo de gerenciamento de risco previsto no PPCOT e apesar de não ter sido mencionado e detalhado no corpo do capítulo IV, do Manual EB- 70-MC-10.307, o exame de situação de contrainteligência prevê o gerenciamento dos riscos levantados, por intermédio da apresentação de linhas de ação para mitigá-los, tanto nos grupos de medidas de segurança orgânica como nos de segurança ativa, utilizando a metodologia descrita no Manual de Contrainteligência.

3 GERENCIAMENTO DE RISCOS

3.1 CONCEITOS GERAIS SOBRE GERENCIAMENTO DE RISCOS

A atividade militar se cerca de riscos inerentes à sua natureza. Por este motivo, a avaliação de risco tornou-se fundamental para o bom desempenho das atividades operacionais, em especial, nas situações de guerra. “O risco pode ter sua origem, tanto no ambiente interno, quanto no externo. Alguns fatores podem dar condições para originar a simples possibilidade do acontecimento de um evento”. (Brasil, 2017b, p. 5-39)

Mas de acordo com Duque (2005), o risco não pode ser eliminado da atividade humana. A única forma de eliminar os riscos seria eliminar a atividade a qual está associado.

No mesmo sentido, Sêmola (2003, p.56) aponta que “é fundamental que todos tenhamos consciência de que não existe segurança total [...]”.

Na atividade militar, genuinamente relacionada às atividades de risco, isto se confirma. Nas lides diárias relacionadas ao serviço, nas atividades de instrução, no manejo de viaturas de combate e administrativas, no trato com assuntos sigilosos, nas diversas oportunidades de interação com a comunidade e o meio ambiente, nos deslocamentos e em outras tantas atividades, pode-se claramente notar a probabilidade de ocorrência de eventos que podem trazer consequências para a operacionalidade da tropa.

Apesar do risco não poder ser eliminado, as vulnerabilidades, as ameaças e os impactos podem ser reduzidos e/ou controlados. É com este objetivo que se analisa e gerencia o risco.

> A gestão de riscos é um processo permanente. A alta administração e gestores responsáveis devem estabelecer, direcionar e monitorar essa gestão, também chamada por gerenciamento. Deve ser aplicada em todos os escalões e prevê atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização ou operação (Brasil, 2018, p. 2-7).

O gerenciamento de risco é um processo contínuo, que não se encerra com a adoção de medidas de segurança. Com a monitoração constante, pode-se identificar as áreas onde não estão sendo alcançados os objetivos e onde há oportunidades de melhoria.

O gerenciamento de risco configura-se então, segundo Brasil (2020, p. 3-17) como “um processo para identificar, avaliar e controlar os riscos associados aos fatores operacionais e à tomada de decisão, bem como a todo o espectro que envolve a atividade militar”. O processo visa buscar o melhor custo-benefício no cumprimento da missão e das atividades diárias.

Dessa forma o gerenciamento de risco vem se tornando uma importante ferramenta para o assessoramento do processo decisório em diversos níveis e atividades desenvolvidas pelo Exército.

Gerenciar riscos é fator decisivo para o sucesso de uma Operação Militar. Segundo o Manual EB- 70-MC-10.307:

> O risco é fator inerente às operações militares, normalmente, está associado à criação de oportunidades para a conquista, retenção e exploração da iniciativa, bem como à obtenção de resultados decisivos (Brasil, 2016).

O conceito de risco operacional é trazido pelo Manual de Doutrina de Operações Conjuntas como “uma ameaça na conquista de um ou mais objetivos da campanha ou operação militar” (Brasil, 2020b, p. 235). Constitui-se em uma combinação de probabilidade e de gravidade dos potenciais danos ao andamento de uma operação, estarão associados à existência de perigos ou ameaças decorrentes de ações adversas advindas das possibilidades do oponente, fatores ambientais e demais incertezas da campanha.

O Processo de Planejamento e Condução das Operações Terrestres (PPCOT), preconiza que o gerenciamento de risco pode levar o decisor a identificar e tratar os riscos inerentes à uma operação militar. Devem ser considerados os riscos de menor impacto, como avaria de material, e os de alto impacto, como perda de vida humana ou comprometimento da missão (Brasil, 2020).

Já no nível de Operações Conjuntas, podemos encontrar importantes considerações sobre o assunto. Segundo Brasil (2020b, p.236), gerenciamento de risco é definindo como “o processo utilizado para administrar os riscos presentes em uma campanha ou operação militar”.

Segundo Brasil (2020b, p. 236), o comandante que for responsável por uma operação deve ter à sua disposição recursos necessários para reduzir ou eliminar os riscos, além de ter liberdade de ação para implementar as medidas para tratamento do risco que julgar necessárias.

A Doutrina de Operações Conjuntas (Brasil, 2020a, p. 169) preconiza que “o Gerenciamento de Risco Operacional (GRO) é uma ferramenta adicional para os comandantes e seus subordinados reduzirem os riscos inerentes às operações”.

3.2 O PROCESSO DE GERENCIAMENTO DE RISCOS

A doutrina de Operações da Força Terrestre e a doutrina de Operações Conjuntas, ambas abordam o gerenciamento do risco dividindo-o em algumas etapas, que se mostram bastante semelhantes nas duas situações.

Primeiramente, na doutrina singular, regida pelo PPCOT, o Processo de Gerenciamento de Risco é iniciado ainda na fase de planejamento, sendo constantemente atualizado nas fases de preparação e execução. Tem a finalidade de evitar a perda significativa do poder de combate, reduzindo a capacidade operativa da tropa amiga.

De acordo com Brasil (2020) o processo para gerenciar os riscos em operações é dividido em seis etapas, são elas: identificar os fatores de risco, avaliar os riscos, selecionar medidas para mitigar os riscos, decidir sobre o risco, implementar medidas de redução dos riscos e supervisionar e avaliar.

Já na doutrina conjunta, conforme Brasil (2020b), este processo é faseado da seguinte forma: identificação das ameaças, avaliação dos riscos decorrentes dos perigos, formulação de medidas para controle do risco, avaliação do risco residual, decisão de risco, implementação de medidas de controle do risco anteriormente levantados e supervisão quanto à eficácia de tais medidas.

Portanto, em breve análise dos dois processos acima descritos, verifica-se que o Manual MD30-M-01 apresenta somente uma diferença com relação ao PPCOT, no que diz respeito ao seu faseamento. Tal diferença consiste na divisão da etapa de decidir sobre o risco, em dois momentos distintos, sendo o primeiro a avaliação do risco residual e o segundo a decisão de qual linha de ação será seguida para tratamento do risco, considerando o risco residual.

Entende-se como risco residual “aquele que permanecerá mesmo após aplicação das ‘medidas de controle’ selecionadas” (Brasil, 2020b, p.236).

Diferentemente do PPCOT, o MD30-M-01 traz o detalhamento de cada etapa, deixando claro que a metodologia do GRO preconizada nas operações conjuntas pode, também, ser aplicada no nível tático.

A primeira etapa, denominada identificação das ameaças, deverão ser considerados os diferentes aspectos dos fatores da decisão: missão, inimigo, área de operações, apoios disponíveis, tempo e espaço. Ainda se analisa as deficiências e vulnerabilidades das próprias Forças e os potenciais danos à população ou à infraestrutura na área das ações, além dos desdobramentos ou impactos para operações futuras.

Ao serem listadas as ameaças, devem ser verificados os impactos possíveis e as causas geradoras de tais impactos. Sob esse aspecto, o *brainstorming* poderá ser uma boa técnica a ser empregada nesse momento" (Brasil, 2020b). A etapa inicial é desenvolvida desde o início do planejamento.

Na segunda etapa realiza-se a avaliação dos riscos decorrentes das ameaças identificadas na fase anterior. São avaliados, também, os impactos negativos para a operação. Para essa avaliação, utiliza-se a ferramenta de matriz da "Probabilidade de ocorrência X Gravidade", cujas entradas são níveis previamente definidos de gravidade e de probabilidade, a partir dos quais se obtém uma classificação padronizada para o risco (Brasil, 2020b).

Na terceira etapa, denominada formulação de medidas de controle de risco, são apresentados procedimentos para a redução de cada risco identificado. Imperativo que se fique claro no planejamento que medida será implementada; quem será o responsável pela sua implementação e acompanhamento; onde será necessária à sua implementação; em que momento da campanha ou operação será implementada; e de que forma ocorrerá essa implementação (Brasil, 2020b). Essas medidas levantadas devem ser lançadas em uma Matriz de Análise do GRO.

Na quarta etapa, denominada avaliação do risco residual, o comandante e seu EM deverão rever a classificação atribuída ao risco após ter considerado o impacto positivo proporcionado pela respectiva medida de controle, obtendo, assim, o chamado "risco residual".

O comandante pode, nesta fase, ordenar uma nova avaliação ou novos tratamentos (linhas de ação) para os riscos apresentados, que também deverão ser lançados na "Matriz de Análise do GRO" (Brasil, 2020b).

Figura 2 - Matriz de Análise do GRO

ANÁLISE DO GRO								
AMEAÇAS À LINHA DE AÇÃO INDICADA								
Nº Evento	Ameaça	Gv	Pbld	Risco	Medidas de Controle do Risco (Que, Onde, Quem, Quando e Como)	Nova Gv	Nova Pbld	Risco Resd
1	Realização de uma Op Anf Ini em uma Ilha do nosso território.	Sev	M Provl	Ctc	a) A FAC deverá realizar, mediante ordem, em coordenação com a FNC, ações de Patrulha Marítima, nas prováveis áreas de desembarque inimigo, antecipando a localização da Força Tarefa Anfíbia inimiga. b) A FNC deverá realizar, mediante ordem, ações de Minagem Defensiva, nas prováveis áreas de desembarque inimigo, diminuindo a probabilidade de sucesso da referida operação inimiga. c) A FTC deverá realizar, mediante ordem, em coordenação com a FAC e FNC, ações de incremento de efetivo de reforço para a ilha, a fim de repelir a ameaça de invasão ao território nacional.	Sev	Provl	Alt

Fonte: Manual MD30-M-01 (Brasil, 2020b).

Na etapa seguinte, o comandante decide se aceita ou não o nível do “risco residual” para aquela campanha/operação. Caso não aceite, formula-se outras medidas de controle adicionais, a modificação da LA, a submissão do risco à apreciação superior ou, até mesmo, a rejeição do risco, o que implicará na adoção de uma nova LA.

Passando à etapa seis, são aplicadas as medidas de controle formuladas e aprovadas pelo comandante, colocando todos os meios e recursos necessários à disposição dos responsáveis pela sua execução.

Na sétima e última etapa é realizado o acompanhamento da efetividade e evolução dessas medidas ou, ainda, das eventuais alterações dessas medidas em relação às ameaças inicialmente identificadas.

Para isso, é de extrema importância que não haja interrupção do fluxo de informações e que o mesmo ocorra de forma oportuna e segura.

> Assim, esse “passo” não se encerra em si, uma vez que a identificação dos riscos é, pois, um procedimento dinâmico que ocorre, em qualquer tempo, ao longo do PPC, guardando as mesmas características daquele processo ao ser cíclico, flexível e contínuo (Brasil, 2020b, p.240).

O processo visa buscar o melhor custo-benefício no cumprimento da missão. Identificar e aceitar riscos de forma prudente é atividade indissociável do exercício da autoridade por meio do Comando e Controle (Brasil, 2014b).

Conclui-se parcialmente que, a metodologia aplicada para o gerenciamento dos riscos nas operações militares em situação de guerra se assemelha ao processo preconizado no exame de situação de contrainteligência, sendo observados diversos

pontos de convergência que facilitam a integração e a complementaridade dos mesmos.

4 A CONTRIBUIÇÃO DO EXAME DE SITUAÇÃO DE CONTRAINTELIGÊNCIA PARA O GERENCIAMENTO DE RISCOS OPERACIONAIS

4.1 ASPECTOS RELEVANTES DA DOUTRINA NORTE-AMERICANA

A Inteligência Militar em operações é de extrema importância para o planejamento e execução dos planos de campanha, especialmente em sua capacidade preditiva. Isso permite que os comandantes mantenham uma consciência situacional contínua (Brasil, 2015).

Nesse escopo, o ramo da contrainteligência cumpre um papel primordial para as Operações Militares. Suas atividades viabilizam a identificação, prevenção e mitigação de ameaças às forças e aos recursos essenciais para as operações, visando preservar o poder de combate e a liberdade de ação.

Tais ameaças podem se valer da negligência de pessoas responsáveis pela salvaguarda de informações e de ações ocasionais promovidas por terceiros, de forma violenta ou não, que gerem prejuízos para a salvaguarda do pessoal, de dados, de informações, de conhecimentos, do material, de áreas ou de instalações (Brasil, 2015).

Nesse sentido, o estudo de situação de contrainteligência contribui para o processo de gerenciamento dos riscos operacionais, pois possibilita a detecção, avaliação e o tratamento de riscos operacionais, abrangendo todos os grupos de medidas, com enfoque voltado para a negação da obtenção de dados e informações por parte do inimigo, bem como na atuação da inteligência adversária.

Dessa forma, cabe fazer uma breve análise de como o tema é tratado na doutrina das Forças Armadas dos Estados Unidos, a fim de identificar boas práticas adotadas. Preliminarmente, cumpre esclarecer que aquele país denomina o conjunto de práticas utilizadas para proteger informações sensíveis e atividades críticas de ameaças internas e externas, como Operações de Segurança (OPSEC). Essas operações selecionam e executam medidas que buscam eliminar o risco das operações ou que as reduzam a um nível aceitável.

De acordo com o manual do Exército dos Estados Unidos da América (EUA), denominado *Operations Security* (USA, 2014), as Operações de Segurança negam aos adversários informações críticas sobre recursos, atividades, limitações e

planejamentos que os adversários precisam para tomar decisões operacionais competentes.

O Exército americano realiza suas Operações de Segurança, aplicando gerenciamento de riscos às Informações Críticas (IC), abrangendo todo o pessoal, missões e atividades conduzidas por eles, especialmente em situação de combate. As medidas de gerenciamento de risco nas OPSEC são realizadas por intermédio de ações efetivas, a fim de alcançar níveis aceitáveis de risco, com os recursos disponíveis.

Nesse contexto, as Operações de Segurança utilizam procedimentos de gerenciamento de riscos para analisar e apoiar as etapas de planejamento, preparação e execução de atividades em diversos cenários militares e ambientes operacionais.

A análise OPSEC visa fornecer aos tomadores de decisão uma ferramenta para avaliar os riscos relacionados às informações críticas que estão dispostos a aceitar durante as operações, enquanto o Gerenciamento de Riscos Operacionais permite que os comandantes avaliem os riscos no planejamento de missões.

No mesmo sentido, o Manual do Estado-Maior Conjunto dos Estados Unidos da América (USA, 2016), determina que os comandantes devem garantir a segurança operacional em todas as fases da operação.

O mesmo manual doutrinário americano descreve que o processo OPSEC é empregado para identificar, controlar e proteger informações críticas e ações que possam ser observadas por sistemas de inteligência adversários. Além disso, ele visa determinar quais dados podem ser coletados, analisados e interpretados pelos adversários, a fim de obter informações relevantes dentro de um prazo que seja útil para eles (USA, 2016).

O processo de gerenciamento de risco adotado nas Operações de Segurança é constituído por cinco fases. Essas fases são aplicáveis a qualquer tipo de Operação, proporcionando uma estrutura sistemática essencial para a identificação, análise e proteção de informações críticas.

Devem ser consideradas as avaliações das vulnerabilidades levantadas em toda a operação, sendo um processo contínuo e cíclico. O *Operations Security - AR*, 530–1 (USA, 2014) descreve as cinco etapas, quais sejam: identificação de informações críticas; análise de ameaças; análise de vulnerabilidades; avaliação de risco e aplicação das contramedidas.

A fim de identificar contribuições que o exame de situação de contrainteligência possa fornecer ao processo de gerenciamento de riscos operacionais, cabe uma breve análise da metodologia norte-americana, aplicada nas Operações de Segurança, para que, ao final, sejam identificadas as semelhanças ou as boas práticas do processo.

A etapa de identificação de informações críticas tem como propósito determinar quais informações necessitam de proteção, tendo em vista que as Operações de Segurança não conseguem proteger todas as informações. É necessário identificar quais devem receber maior atenção e esforço para sua salvaguarda. O Oficial de Inteligência desempenha um papel fundamental, devendo fornecer informações sobre o inimigo, suas capacidades, limitações e intenções, tudo com o objetivo de identificar as informações críticas amigas (USA, 2014).

Na etapa de análise de ameaças, segundo *Operations Security* - AR, 530–1 (USA, 2014), ocorre a identificação de capacidades que o inimigo possui para coletar informações críticas das Forças Amigas. Para essa etapa, são analisadas todas as fases da operação e todas as funções de combate, sendo que as informações críticas levantadas são confrontadas com as capacidades de coleta da inteligência adversária. Após esse confronto, sendo encontrada uma correspondência, há uma vulnerabilidade.

Na etapa seguinte, a análise de vulnerabilidades, ocorre a identificação de cada vulnerabilidade e a elaboração de medidas, mesmo que provisórias, para mitigar essas vulnerabilidades. As medidas propostas devem ser eficientes e eficazes para lhe dar com a vulnerabilidade encontrada e se dividem em três categorias.

A primeira é o controle da ação. Nessa categoria as medidas visam agir nas atividades das Forças Amigas, eliminando ou reduzindo a vulnerabilidade que pode ser identificada e explorada pela Inteligência adversa. A segunda categoria se refere a medidas que dificultam ou impedem a coleta de informações pelo inimigo. A terceira categoria, por sua vez, se volta para o analista de inteligência adversário e tem por finalidade evitar interpretações precisas das vulnerabilidades por intermédio de dissimulações (USA, 2014).

A quarta etapa do gerenciamento do risco nas OPSEC é a avaliação do risco. Nessa etapa, as medidas a serem implementadas são submetidas à apreciação do comandante, que decide sobre efetivá-las ou não. São avaliados os impactos da

medida nas Operações correntes e futuras, além do risco ou impacto, caso uma medida não seja implementada.

A avaliação de risco é realizada com base em uma estimativa da capacidade do inimigo de explorar uma vulnerabilidade, bem como nos potenciais impactos ou efeitos que essa exploração pode ter nas operações. Nesse sentido, são levantadas medidas para controlar a exposição de informações críticas ao inimigo.

A última etapa do gerenciamento de risco consiste na aplicação de medidas e contramedidas. Destina-se à aplicação das medidas aprovadas pelo comandante nas operações correntes e nas operações futuras

Da análise de toda a metodologia empregada nas Operações de Segurança do Exército dos EUA, conclui-se parcialmente que o processo apresenta semelhanças com o exame de situação de contrainteligência, principalmente no que diz respeito à análise e tratamento dos riscos.

4.2 ASPECTOS RELEVANTES DA DOUTRINA BRASILEIRA

Após realizada uma análise do exame de situação de contrainteligência e do gerenciamento dos riscos operacionais nos capítulos anteriores, nesta Seção serão comparadas as etapas dos dois processos, no intuito de alcançar o objetivo proposto por este estudo.

A fim de enriquecer ainda mais a avaliação, serão apontadas as correspondências com as Operações de Segurança do Exército americano, identificando as lições aprendidas. Da análise das OPSEC na doutrina dos EUA, verifica-se alguns pontos de convergência com a doutrina brasileira, que podem auxiliar no levantamento das contribuições que o exame de situação de contrainteligência pode oferecer para o gerenciamento dos riscos operacionais.

A primeira etapa do exame de situação de contrainteligência, onde são levantadas as principais ameaças e vulnerabilidades envolvidas na operação, se coaduna com a primeira fase do gerenciamento de riscos, denominada identificação das ameaças e com a primeira fase das OPSEC, denominada identificação de informações críticas. Nesta etapa, a contrainteligência auxilia na identificação dos principais ativos a serem protegidos, classificando-os de acordo com os grupos de medidas da segurança orgânica e ativa (Brasil, 2016).

“As fontes de informações para a identificação das ameaças deverão incluir o

reconhecimento das áreas de operação, as operações de inteligência, a experiência do comandante e do seu EM, entre outras” (Brasil, 2020b, p.238).

A segunda etapa do exame de situação de contrainteligência, que visa identificar aspectos da área de operações que são passíveis de serem explorados pelas ameaças, complementa as informações necessárias para a primeira etapa do processo de gerenciamento de riscos operacionais, ao passo que levanta vulnerabilidades relativas às Forças Amigas, Forças Inimigas, Terreno, Condições Meteorológicas e Considerações Civis.

Na terceira e quarta etapa do exame de situação de contrainteligência é realizada uma avaliação das atividades e capacidades inimigas, particularmente no que tange à possibilidade de suas diversas fontes de inteligência em obter informações ou detectar vulnerabilidades das Forças Amigas. Tais etapas encontram similaridade com a segunda fase das Operações de Segurança do Exército dos EUA, uma vez que nessa fase da OPSEC busca-se identificar a capacidade de coleta da inteligência inimiga.

Portanto, as quatro primeiras etapas do exame de situação de contrainteligência contribuem sobremaneira com as informações necessárias à primeira fase do processo de gerenciamento de riscos e abrangem objetivos semelhantes às duas primeiras fases das OPSEC americanas.

Finalizada as quatro primeiras etapas do exame de situação de contrainteligência, inicia-se a fase de avaliação do risco, regida pelo Manual de Contrainteligência, que em muito se assemelha ao processo de gerenciamento de riscos operacionais, conforme análise a seguir.

A fase de avaliação do risco, no escopo do exame de situação de contrainteligência, tem início com classificação dos riscos levantados anteriormente de acordo com o grau de probabilidade de ocorrência e impacto sobre as linhas de ação adotadas na Operação Militar. Em seguida, os riscos são classificados em níveis (baixo, médio, alto e extremo) e agrupados de acordo com o grupo de medidas correspondente, a fim de auxiliar na tomada de decisão para o tratamento dos riscos.

Com isso, de uma maneira bem clara, verifica-se a semelhança da fase de avaliação do risco do exame de situação de contrainteligência, com a fase dois do processo de gerenciamento de riscos, denominada avaliação dos riscos decorrentes.

Em ambos os processos, a metodologia da matriz probabilidade x impacto se faz presente, o que facilita a integração das informações levantadas.

Na sequência do exame de situação de contrainteligência, logo após a avaliação dos riscos, são elaboradas linhas de ação para o seu tratamento, que decorre das seguintes possibilidades: aceitar, compartilhar, evitar ou mitigar os riscos. Neste diapasão, observando a fase três do processo de gerenciamento de risco, denominada formulação de medidas de controle do risco, verifica-se convergência dos processos, uma vez que as fases descritas acima apresentam a mesma finalidade, ou seja, a formulação de medidas/linhas de ação para tratar os riscos.

Fazendo um paralelo com as OPSEC, verifica-se que na fase de análise das vulnerabilidades também ocorre a elaboração de medidas, portanto, observa-se correspondência com a doutrina brasileira.

A última fase da avaliação do risco no exame de situação de contrainteligência, denominada decisão, encontra uma fase equivalente no processo de gerenciamento de riscos, que se denomina decisão de risco. Em ambas as fases o Comandante decide pela linha de ação ou medida a ser adotada ou se vai aceitar o risco residual ou integralmente.

Da mesma forma ocorre nas Operações de Segurança dos EUA, onde em sua quarta etapa, o Comandante da Operação aprecia a medidas formuladas para a mitigação dos riscos e decide se vai efetivá-las ou não.

De tudo o que foi exposto no presente capítulo, conclui-se parcialmente que os processos analisados possuem diversas semelhanças que contribuem para a integração entre eles. A similaridade da metodologia empregada assegura que as ameaças levantadas no exame de situação de contrainteligência podem complementar o processo de gerenciamento de riscos operacionais em situação de guerra.

5 CONCLUSÃO

As Operações Militares sofreram significativas mudanças nos últimos anos. Uma das principais características da guerra moderna é a utilização de tecnologias avançadas, como sistemas de comunicação e informação, drones, ciberataques e armas de alta precisão. Essas tecnologias têm um impacto significativo no combate, permitindo uma maior capacidade de monitoramento, coleta de informações, coordenação e execução de ataques precisos.

O surgimento de atores não estatais com relativa capacidade de interferir no resultado de uma campanha militar trouxe novas ameaças, e por consequência, novos riscos ao Campo de Batalha. As operações de amplo espectro, estão exigindo dos exércitos, adaptações de técnicas, táticas e procedimentos para se adequarem a um ambiente cada vez mais complexo.

Nesse ambiente dinâmico, elevou-se os níveis de risco das operações, e por conseguinte, trouxe a necessidade de maior refinamento do planejamento, integrando-o cada vez mais ao gerenciamento dos riscos operacionais envolvidos.

Para alcançar a cobertura de toda a variedade de ativos existentes em uma Operação, o exame de situação de contrainteligência se mostra uma ferramenta eficaz, sendo uma das suas principais características, a divisão em grupos de medidas. Tal divisão, já consagrada na doutrina brasileira vigente, facilita a identificação e até mesmo a formulação de medidas de tratamento do risco.

Da análise das etapas e da metodologia empregada pode-se concluir que o exame de situação de contrainteligência contribui para o processo de gerenciamento de risco operacional em situação de guerra, em diversos aspectos. Primeiramente, por meio dele, é possível a identificação e avaliação das ameaças provenientes da inteligência inimiga, bem como suas capacidades, intenções e atividades, permitindo que o comandante e seu Estado-Maior compreendam os riscos e as vulnerabilidades enfrentadas e possam adotar medidas apropriadas para mitigá-los.

Durante o referido processo é possível, ainda, identificar a possibilidade do inimigo em realizar atividades de espionagem, sabotagem e outras ações adversas que podem afetar diretamente as Operações Militares.

No que diz respeito à proteção das informações, o exame de situação de contrainteligência desempenha uma tarefa semelhante às Operações de Segurança

adotadas na doutrina norte-americana, contribuindo para a proteção de informações sensíveis, como planos de campanha, evitando que sejam descobertos pelo inimigo.

A segurança da informação, sendo um dos grupos de medidas do Segmento da Segurança Orgânica, é trabalhado desde os tempos de paz, à semelhança do que ocorre com as OPSEC nos EUA.

Importante frisar que as OPSEC têm como foco principal a informação crítica e seus indicadores, que seriam os dados isolados da informação. O exame de situação de contrainteligência tem maior amplitude na Operação Militar, pois foca em outros ativos nela envolvidos, sendo, a segurança da informação um dos grupos de medida trabalhados no processo.

A contrainteligência fornece uma perspectiva valiosa sobre as atividades do inimigo, suas redes de agentes e sua coleta de informações. Isso permite uma avaliação mais precisa da probabilidade e do impacto dos riscos operacionais, contribuindo com a formulação de linhas de ação mais eficientes e com maior segurança.

Além disso, a contrainteligência contribui para o gerenciamento de risco operacional ao fornecer recomendações e medidas de proteção para reduzir as vulnerabilidades e aumentar a resiliência das Forças Amigas. Isso pode envolver a implementação de medidas de segurança física, segurança da informação, dos recursos humanos, do material, segurança cibernética e contraespionagem, bem como ações para desinformar o inimigo e proteger as comunicações.

O principal objetivo da Contrainteligência é investigar além do óbvio. Sua abrangência deve ser ampla o bastante para analisar minuciosamente os detalhes de uma ameaça, ao mesmo tempo em que é necessário ter uma visão de longo prazo para compreender o impacto que a exploração de uma vulnerabilidade pelo inimigo pode causar na Operação.

Ao considerar o exame de situação de contrainteligência como ferramenta capaz de fornecer subsídios para o processo de gerenciamento de risco das Operações Militares, é possível reduzir esses riscos e aumentar a segurança das Forças em campanha.

A compreensão dessa dinâmica e o entendimento das contribuições que o exame de situação de contrainteligência pode prestar ao gerenciamento de riscos operacionais, conforme elencadas nessa seção, são essenciais para o

desenvolvimento de estratégias militares eficazes e para a proteção das forças envolvidas no ambiente complexo dos conflitos contemporâneos.

REFERÊNCIAS

BRASIL. Exército Brasileiro. Comando do Exército. **Contrainteligência**. EB70-MC-10.220. 1. ed. Brasília, DF, 2019.

BRASIL. Exército Brasileiro. Comando do Exército. **Diretriz Reguladora da Política de Gestão de Riscos do Exército Brasileiro.** EB20-D-02.010. 1. ed. Brasília, DF, 2019.

BRASIL. Exército Brasileiro. Comando do Exército. **Instruções Gerais para as Publicações Padronizadas do Exército**. EB10-IG-01.002. 1. ed. Brasília, DF, 2011.

BRASIL. Exército Brasileiro. Comando do Exército. **Inteligência**. EB20-MC-10.207. 1. ed. Brasília, DF, 2015.

BRASIL. Exército Brasileiro. Comando do Exército. **Inteligência Militar Terrestre**. EB20-MF-10.107. 2. ed. Brasília, DF, 2015.

BRASIL. Exército Brasileiro. Comando do Exército. **Manual Técnico da Metodologia de Riscos do Exército Brasileiro.** EB20-MT-02.001. 1. ed. Brasília, DF, 2019.

BRASIL. Exército Brasileiro. Comando do Exército. **Metodologia da Política de Gestão de Riscos do Exército Brasileiro.** EB20-D-07.089. 1. ed. Brasília, DF, 2017.

BRASIL. Exército Brasileiro. Comando do Exército. **Operações**. EB70-MC-10.223. 5. ed. Brasília, DF, 2017.

BRASIL. Exército Brasileiro. Comando do Exército. **Planejamento e Emprego da Inteligência Militar**. EB70-MC-10.307. 1. ed. Brasília, DF, 2016.

BRASIL. Exército Brasileiro. Comando do Exército. **Política de Gestão de Riscos do Exército Brasileiro** EB10-P-01.004. 2. ed. Brasília, DF, 2018

BRASIL. Exército Brasileiro. Comando do Exército. **Processo de Planejamento e Condução das Operações Terrestres**. EB20-MC-10.211. 2. ed. Brasília, DF, 2020.

BRASIL. Exército Brasileiro. Comando do Exército. **Produção do conhecimento de Inteligência**. EB70-MT-10.401. 1. ed. Brasília, DF, 2019.

BRASIL. Ministério da Defesa. **Estado-Maior Conjunto das Forças Armadas.** MD30-M-01: Doutrina de Operações Conjuntas – 1º Volume. 2. Ed. Brasília, DF, 2020.

BRASIL. Ministério da Defesa. **Estado-Maior Conjunto das Forças Armadas.** MD30-M-01: Doutrina de Operações Conjuntas – 2º Volume. 2. Ed. Brasília, DF, 2020.

CRESWELL, John W. **Projeto de pesquisa: métodos qualitativo, quantitativo e misto**; tradução Magda Lopes. – 3 ed. – Porto Alegre, RS, 2010.

ESTADOS UNIDOS DA AMÉRICA. **Joint Publication (JP) 3-13.3:** Operations Security (OPSEC). Manual do Estado-Maior Conjunto dos Estados Unidos da América, 2016.

ESTADOS UNIDOS DA AMÉRICA. **Army Regulation 530-1:** Operations Security. Manual do Exército dos Estados Unidos da América, Washington DC, 2014.

GALLAGHER, Brendan Gerenciamento de Risco no Exército de Hoje. **Military Review**, Fort Leavenworth, p. 20-27, Março – Abril, 2014.

RAMOS, Renato Augusto Lyrio. O emprego da contrainteligência militar no planejamento e execução das operações militares em situação de guerra. **Revista Lucerna**,n. 11, p.57-69, Brasília, 2022.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**. Rio de Janeiro. Campus, 2003.