O EMPREGO DA CONTRAINTELIGÊNCIA MILITAR NO PLANEJAMENTO E EXECUÇÃO DAS OPERAÇÕES MILITARES EM SITUAÇÃO DE GUERRA

Renato Augusto Lyrio dos Ramos[1]

Resumo: O Exército Brasileiro possui, em sua doutrina, o Gerenciamento do Risco Operacional. Nele está descrito o processo de identificação e tratamento do risco, porém, sem detalhar cada etapa. O Exército Norte-americano também possui, em sua doutrina, seu Gerenciamento de Risco. Neste trabalho, o gerenciamento descrito é o que se executa nas Operações de Segurança (OPSEC). As OPSEC se assemelham ao grupo de medidas de Segurança da Informação, na Segurança Orgânica, segmento da Contrainteligência. Os objetivos do trabalho são realizar uma comparação entre os processos de gerenciamento de risco em operações militares entre as doutrinas citadas e apresentar uma sugestão de facilitação do processo já existente na doutrina brasileira. Na conclusão, verifica-se que há mais semelhanças do que diferenças em ambas as doutrinas estudadas. Nota-se as diferenças, principalmente, devido ao objetivo final de cada processo, uma é focada nos ativos envolvidos numa operação, enquanto outra é voltada exclusivamente para a informação crítica. Ainda na conclusão, é apresentada uma sugestão de nova Matriz Avaliação do Risco e Linhas de Ação, a ser executada em operações, considerando, inclusive, a fase de planejamento. Conclui-se com a necessidade de aperfeiçoamento da doutrina brasileira, com inclusão de OPSEC como operação ininterrupta, mesmo em tempo de paz e revisão do processo de gerenciamento de risco em vigor.

Palavras-chave: Gerenciamento de Risco. Operações de Segurança. Contrainteligência. Doutrina. Operações Militares.

Abstract: The Brazilian Army has, in its doctrine, Operational Risk Management. It describes the process of risk identification and treatment, however, without detailing each step. The US Army also has, in its doctrine, its Risk Management. In this work, the management described is what is performed in Security Operations (OPSEC). OPSEC is similar to the Information Security measures group, in Organic Security, Counterintelligence segment. The objectives of the work are to carry out a comparison between the risk management processes in military operations among the cited doctrines and to present a suggestion of facilitation of the process already existing in the Brazilian doctrine. In conclusion, it appears that there are more similarities than differences in both doctrines studied. Differences are noted, mainly due to the final objective of each process, one is focused on the assets involved in an operation, while the other is focused exclusively on critical information. Still in the conclusion, a suggestion is presented for a new Risk Assessment Matrix and Lines of Action, to be implemented in operations, including the planning phase. It concludes

[1] TC de Comunicações do Exército Brasileiro - Academia Militar das Agulhas Negras. Pós-graduado em Gestão em Administração Pública – Centro Universitário Leonardo da Vinci. Pós-graduado em Operações Militares - Escola de aperfeiçoamento de Oficiais. Pós-graduado em Segurança da Informação – Universidade Estácio. Pós-graduado em Gestão de Organizações de Inteligência – Escola de Inteligência Militar do Exército.

with the need to improve Brazilian doctrine, with the inclusion of OPSEC as an uninterrupted operation, even in peacetime, and a review of the risk management process in place.

Keywords: Risk management. Security Operations. Counter-intelligence. Doctrine. Military Operations.

1 INTRODUÇÃO

O Manual EB70-MC-10.220, Contrainteligência (BRASIL, 2019c, p. 1-1), reporta o conceito de Contrainteligência. Ela é um ramo de toda a atividade de Inteligência Militar que possui verbos que norteiam sua missão. Prevenir, detectar, identificar, avaliar, obstruir, explorar e neutralizar as ações da Inteligência adversa ou de qualquer natureza, desde que constituam ameaça à salvaguarda dos ativos que o Exército Brasileiro (EB) tenha interesse de proteger. Esses ativos são dados, conhecimentos, áreas, instalações, pessoas e meios.

Segundo o manual do Exército Norte-americano *Operations Security* (*Army Regulation 530–1*, 2014, p. 1), as Operações de Segurança (OPSEC) negam aos adversários informações críticas sobre recursos, atividades, limitações e intenções amigas que os adversários precisam para tomar decisões operacionais competentes. Além disso, essas operações selecionam e executam medidas que buscam eliminar o risco das operações ou que as reduzam a um nível aceitável.

O Guia de Segurança de Operações (OPSEC) (*RCC Document 600-11*, 2011, p. vii), que regula a atividade de OPSEC no *Range Commanders Council* (RCC), nos Estado Unidos da América (EUA), preconiza que já existem programas e procedimentos de segurança para proteger assuntos confidenciais. Mas, nota-se que as informações, geralmente disponíveis ao público, podem conter dados que revelem a existência e, por vezes, pormenores sobre informações classificadas ou sensíveis.

Continua, ainda, destacando a importância da proteção de indicadores que auxiliem ou exponham informações chamadas de críticas àqueles que buscam neutralizar ou explorar as ações do governo dos EUA na área de segurança nacional.

O Processo de Planejamento e Condução das Operações Terrestres (PPCOT), (BRASIL, 2020, p. 3-17) 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.

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

Segundo Brasil (2020b, p. 169), 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.

No âmbito do EB, ainda não há manuais ou publicações doutrinárias que abordem, de maneira detalhada, gerenciamento de risco em Operações Militares de Guerra e como esse gerenciamento pode se tornar uma ferramenta efetiva para a Contrainteligência nesse ambiente.

Gerenciar riscos é fator decisivo para o sucesso de uma Operação Militar. O EB preconiza esse gerenciamento em manuais, como no EB70-MC-10.211 (Processo de Planejamento e Condução da Operações Terrestres). O Exército dos Estados Unidos da América (EUA) conduz suas Operações de Segurança (OPSEC), com gerenciamento de risco aplicável às Informações Críticas (IC), no âmbito de todo o pessoal, missões e atividades por eles executados.

As medidas de gerenciamento de risco vão ao encontro das OPSEC, sendo preconizado a orientação do comandante e as ações efetivas a fim de se obter níveis aceitáveis de risco, com a utilização de recursos disponíveis.

2 O GERENCIAMENTO DE RISCO EM OPERAÇÕES MILITARES

A Política de Gestão de Riscos do Exército Brasileiro (BRASIL, 2018, p. 3-7) define risco como uma possibilidade de ocorrência de um evento que trará um impacto no cumprimento dos objetivos que a instituição estabeleceu. Complementa que o risco deve ser, por exemplo, medido em termos de probabilidade e impacto.

O manual de OPSEC da Marinha norte-americana (NTTP 3-13.3M/MCTP 3-32B, 2017) possui uma definição mais simples, sendo o risco a probabilidade e gravidade da perda ligada a perigos. Pode-se entender a gravidade como o impacto decorrido pelo evento e o perigo como uma fonte ou uma situação com potencial para provocar danos.

A gestão de riscos, segundo BRASIL (2018, p. 2-7), 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.

Nesse sentido, a Diretriz Reguladora da Política de Gestão de Riscos do Exército Brasileiro - EB20-D-02.010 (BRASIL, 2019b, p. 4-14), indica que a avaliação de riscos deve ocorrer sob a perspectiva de probabilidade e impacto de sua ocorrência, além do inter-relacionamento com outros riscos. Deve-se considerar a condição de riscos inerentes ou residuais.

Entende-se como risco operacional toda ameaça encontrada nas ações de conquista de um ou mais objetivos da campanha ou operação militar, podendo ocorrer mais de uma causa para ocasionar o risco. Qualquer fato, ato ou condição, seja ela potencial ou não, podem gerar probabilidade de ocorrência de impactos nos objetivos estabelecidos, criando insegurança nas ações. (BRASIL, 2020a, p. 235)

Ainda, segundo BRASIL (2020a, p. 236), os riscos existentes em uma campanha ou operação militar devem ser gerenciados por um processo. Este processo deve compreender as fases de identificação das ameaças, da avaliação dos riscos decorrentes dos perigos, da formulação de medidas para controle do risco, da avaliação do risco residual, da decisão de risco (quando o comandante decide se aceita ou não o risco residual), da implementação de medidas de controle do risco anteriormente levantados e da supervisão quanto à eficácia de tais medidas.

No mesmo sentido, as OPSEC preconizam etapas de gerenciamento de risco para examinar e auxiliar as fases de planejamento, preparação, execução e pós-execução de qualquer atividade em todo o espectro de ações militares e ambientes operacionais. A análise OPSEC tem a finalidade de fornecer aos decisores um meio de avaliação dos riscos inerentes às informações críticas que estarão dispostos a

aceitar em operações, da mesma forma que o GRO permite que os Comandantes avaliem o risco no planejamento da missão.

A NTTP 3-13.3M/MCTP 3-32B (2017, p. 179) define informação crítica como qualquer dado específico sobre intenções, capacidades e atividades de tropas amigas que são necessárias para que os adversários planejem e ajam de forma eficaz, garantindo o fracasso ou consequências inadmissíveis para o cumprimento da missão amiga.

2.1 GERENCIAMENTO DE RISCO EM OPERAÇÕES MILITARES, SEGUNDO A DOUTRINA DO EXÉRCITO BRASILEIRO

O risco pode ter sua origem, segundo BRASIL (2017b, p. 5-39), tanto no ambiente interno, quanto no externo. Alguns fatores podem dar condições para originar a simples possibilidade do acontecimento de um evento.

O Manual EB70-MC-10.223, Operações (BRASIL, 2017a, p. 2-1) 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. Destaca que a Operação é realizada desde a paz, em amplo espectro, até o conflito propriamente dito (armado).

Como ação preventiva, a Segurança Orgânica, segmento da Contrainteligência que tem como foco a proteção dos ativos (recursos humanos, informação, instalações, material e áreas e instalações), apresenta o ciclo contínuo de medidas, que passam pelo planejamento, execução, controle e realimentação. Todos os integrantes do Exército, seja militar ou civil, estão envolvidos com este ciclo (BRASIL, 2019c, p. 3-1).

Para atingir a proteção da amplitude de ativos existentes no EB, a Segurança Orgânica é dividida em grupos de medidas, são eles: Segurança dos Recursos Humanos, Segurança do Material, Segurança das Áreas e Instalações e Segurança da Informação. A divisão dos ativos nesses grupos facilita a execução das avaliações de riscos, evitando excesso ou insuficiência de medidas (BRASIL, 2019c, p. 3-2).

Houve uma mudança no contexto das operações militares desde os anos 90. Surgiram atores não estatais que possuem relativa capacidade de interferir no resultado de uma campanha militar. Estão inseridos em ambientes urbanos, dissimulados entre a população civil, exigindo dos exércitos, adaptações de técnicas, táticas e procedimento (TTP) para se adequarem a um ambiente mais complexo. Novos riscos surgiram atrelados às operações de amplo espectro (BRASIL, 2020, p. 1-3).

Nesse sentido, o Manual EB70-MC-10.220, Contrainteligência (BRASIL, 2019c, p. 5-1) apresenta o Planejamento de Contrainteligência. Salienta que todo militar possui responsabilidades para com a proteção da Força. Comportamentos, atitudes preventivas, adoção de medidas protetivas efetivas e proativas auxiliam na diminuição ou prevenção aos riscos.

Para a execução do Planejamento de Contrainteligência, BRASIL (2019c, p. 5-2) divide seu desenvolvimento em duas fases: o Exame de Situação e o Processo de Desenvolvimento da Contrainteligência (PDCI). O Exame de Situação apresenta uma sequência ordenada de fatores que auxiliarão no processo decisório que estiver relacionado à Contrainteligência. O PDCI está diretamente relacionado às atividades para solucionar falhas ligadas às vulnerabilidades da Organização Militar.

Na mesma direção, o Manual EB70-MC-10.307, Planejamento e Emprego de Inteligência Militar (BRASIL, 2016, p. 4-2) apresenta o conceito de Planejamento de Contrainteligência. O foco do planejamento deve estar nas possibilidades das forças inimigas em obter conhecimentos, dados, informações sensíveis ou críticas, além das atividades de espionagem, sabotagem, terrorismo, propaganda adversa e desinformação.

Segundo Brasil (2016, p. 4-2), o Exame de Situação de Contrainteligência, a fim de verificar a probabilidade e impacto das possibilidades de ação da Inteligência inimiga, faz uma avaliação da eficiência das medidas de Contrainteligência empregadas para conter essa ação, inserindo o gerenciamento do risco em seu relatório final (p. I-1).

Deve ser feita uma avaliação criteriosa das possibilidades das fontes de Inteligência inimiga. Determinar a capacidade de exploração das vulnerabilidades das tropas amigas e as possibilidades de efeitos negativos sobre as linhas de ação amigas (BRASIL, 2016, p. 4-5).

O PPCOT (BRASIL, 2020, p. 3-17) vai ao encontro do preconizado no MD30-M-01, Doutrina de Operações Conjuntas (BRASIL, 2020b) no que tange ao Processo de Gerenciamento de Risco. Ele é iniciado ainda na fase de planejamento e deve ser 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. A célula de operações de médio prazo ou a seção de planejamento deve coordenar a execução do GRO.

Desta forma, Brasil (2020, p. 3-17) divide o processo para gerenciar os riscos em operações 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. Ele explica sucintamente como é cada etapa, deixando claro que a metodologia do GRO preconizada nas operações conjuntas pode, também, ser aplicada no nível tático.

O Manual MD30-M-01 (BRASIL, 2020b, p. 236) orienta o GRO com etapas semelhantes. Ele divide a 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.

Sobre o GRO, Brasil (2020b, p. 238) o descreve como um processo cíclico e contribui diretamente para o êxito da missão. A fase de identificação das ameaças deve incluir, inclusive, as deficiências e vulnerabilidades da exposição de informações da própria força amiga.

Deve ser realizada a avaliação dos riscos decorrentes das ameaças identificadas na fase anterior. Serão avaliados, também, os impactos negativos para a operação. Para essa avaliação, utiliza-se a ferramenta de matriz da “Probabilidade de ocorrência X Gravidade”, obtendo uma classificação final sobre a gravidade do risco (BRASIL, 2020b, p. 239).

Brasil (2020b, p. 239) continua com a fase da formulação de medidas de controle de risco. É necessário, nesta fase, apresentar procedimentos de redução de cada risco identificado. Deve-se responder perguntas como: Que medida será implementada? Quem será o responsável pela sua implementação e acompanhamento? Onde, quando e de que forma será a implementação?

Feito isso, é realizada a avaliação do risco residual e a decisão do comandante se aceita ou não os riscos para a operação. O comandante pode, nesta fase, ordenar uma nova avaliação ou novos tratamentos (linhas de ação) para os riscos apresentados (BRASIL, 2020b, p. 240). Ele ordena a implementação das

medidas e determina seu acompanhamento, a fim de manter-se atualizado para intervenção oportuna.

2.2 GERENCIAMENTO DE RISCO EM OPERAÇÕES MILITARES, SEGUNDO A DOUTRINA DO EXÉRCITO NORTE-AMERICANO

Joint Publication (JP) 3-13.3, *Operations Security (OPSEC),* Manual do Estado-Maior Conjunto dos Estados Unidos da América (JP 3-13.3, 2016), traz, ainda em sua visão geral, que os comandantes devem garantir a segurança operacional (Operação de Segurança – OPSEC) em todas as fases da operação.

JP 3-13.3 (2016, p. vii) define que o processo OPSEC, sendo sistemático, deve ser usado para identificar, controlar e proteger as informações críticas e ações que podem ser observadas por sistemas de inteligência adversários. Deve, também, determinar quais dados podem ser coletados, analisados e interpretados para obter informações a tempo de serem úteis aos adversários.

NTTP 3-13.3M/MCTP 3-32B (2017, p. 21) complementa que a OPSEC é uma capacidade relacionada à informação. Ao ser bem empregada, pode auxiliar na obtenção de vantagens no ambiente informacional, cabendo ao comandante incorporá-la às operações. Para isso, o comando inclui um gerente ou coordenador e um grupo de trabalho do programa OPSEC, devendo ser nomeados em documentação oficial.

Na mesma direção, *RCC Document 600-11* (2011, p. 2-1) descreve, como um dos objetivos da OPSEC, a identificação de informações e atividades observáveis relacionadas a capacidades da missão, limitações e intenções da força amiga a fim de evitar a exploração pelos adversários. A identificação e proteção dessas informações críticas são um meio positivo e proativo para negar a vantagem ao inimigo.

Sobre informações críticas, *Operations Security* - AR (530–1, 2014, p. 1) as define como sendo as informações importantes para a realização exitosa de objetivos e missões amigas, ou que podem ser úteis para um adversário. Elas consistem em dados sobre capacidades, limitações e intenções amigas que podem ser exploradas por adversários para planejar e executar ações efetivas de modo a degradar o cumprimento da missão de tropas amigas.

De forma semelhante, NTTP 3-13.3M/MCTP 3-32B (2017, p. 3-2) detalha que as informações críticas são atividades, intenções, capacidades ou limitações amigas que um adversário procura na intenção de obter vantagem militar, política, diplomática, econômica ou tecnológica. Destaca que as informações críticas podem envolver alguns indicadores de informações sobre atividades ou intenções amigas que, ao serem expostas, podem degradar significativamente a eficácia da missão. Nota-se que informações que são críticas em uma fase da missão podem não ser críticas nas fases subsequentes.

Segundo NTTP 3-13.3M/MCTP 3-32B (2017, p. 3-3), os indicadores OPSEC e as informações críticas são analisados de forma conjunta. Eles são definidos como dados encontrados em fontes abertas que podem ser reunidos e interpretados, gerando uma informação útil ao elemento hostil, sejam elas críticas, vulnerabilidades e, até mesmo, confidenciais.

O Manual norte-americano *Operations Security* - AR, 530–1 (2014, p. 2) deixa claro que as OPSEC fornecem uma metodologia para gerenciar os riscos inerentes à informação, mas que é impossível evitar todos eles e proteger todos os ativos.

Segundo *Operations Security* - AR, 530–1 (2014, p. 22), o processo de gerenciamento de risco preconizado nas OPSEC é composto por cinco fases. Elas podem ser aplicadas em qualquer plano, operações ou atividades, fornecendo uma estrutura sistemática necessária para identificar, analisar e proteger informações críticas.

Deve ser considerada a natureza mutável das informações críticas, a própria ameaça e as avaliações das vulnerabilidades realizadas em toda a operação. É um processo contínuo e cíclico, devendo ocorrer durante toda a operação. *Operations Security* - AR, 530–1 (2014, p. 23) descreve as cinco etapas, sendo elas: identificação de informações críticas; análise de ameaças; análise de vulnerabilidades; avaliação de risco e aplicação das contramedidas medidas OPSEC.

A fase de identificação de informações críticas tem como objetivo determinar quais informações precisam de proteção. Como citado anteriormente, as OPSEC não podem proteger tudo. Deve ser identificado quais itens devem receber maior atenção e esforço para sua proteção. O Oficial de Inteligência deve fornecer informações sobre o inimigo, suas capacidades, limitações, intenções, tudo com a finalidade de levantar informações críticas amigas (*Operations Security* - AR, 530–1, 2014, p. 23).

Alguns exemplos de informações críticas podem ser abordados, porém, *Operations Security* - AR, 530–1 (2014, p. 26) destaca que uma lista de verificação pode não ser eficaz, uma vez que cada operação ou atividade tem informações críticas exclusivas, sendo necessária uma avaliação específica para cada atividade ou operação. Regras de engajamento, dispositivo no terreno, características e capacidades específicas de armas e sistemas eletrônicos, capacidade da Inteligência e Contrainteligência, novos sistemas de armas, todas são informações críticas.

A etapa de análise de ameaças, segundo *Operations Security* - AR, 530–1 (2014, p. 24), tem como finalidade a identificação de recursos que a força adversa possui para coletar informações críticas amigas. A atividade de coleta hostil visa ações e informações abertas ou disponíveis para obter indicadores que impactarão negativamente a missão.

Para essa etapa, a equipe OPSEC e de Inteligência devem examinar todas as fases da operação, a fim de identificar ações ou informações que destacam os indicadores em cada área de pessoal, logística, comunicações, movimento de tropas, aviação, etc. Os indicadores encontrados devem ser confrontados com as capacidades de coleta da inteligência adversária. Essa ação fica facilitada ao se montar uma “linha do tempo da missão”, identificando, ao longo da linha, tudo que se deseja proteger (*Operations Security* - AR, 530–1, 2014, p. 24).

AR 530–1 (2014, p. 24) prossegue a descrição da etapa ao indicar que devem ser levantadas, ao longo da linha do tempo, as ações que devem ser realizadas para que a missão seja cumprida e quais dessas ações também são indicadores. Ao se comparar o indicador com a capacidade de coleta do inimigo e sendo encontrada uma correspondência, neste indicador há uma vulnerabilidade.

A etapa seguinte é a análise de vulnerabilidades. AR 530–1 (2014, p. 24) expressa o objetivo dessa análise como a identificação de cada vulnerabilidade e a elaboração de medidas, ainda que provisórias, para lidar com essas vulnerabilidades. Cita que proteção adequada com menor custo, mas sendo suficientemente eficiente e eficaz, é a mais desejável.

É possível reunir as medidas a serem executadas em três categorias. A primeira é o controle da ação. Nessa categoria devem ser previstas medidas para controlar as atividades amigas, eliminando ou reduzindo indicadores ou a vulnerabilidade que pode ser notada pela Inteligência adversa. AR 530–1 (2014, p. 24) cita que devem ser especificadas, nas medidas, quem, quando, onde e como.

A segunda categoria reúne medidas que impedem a coleta de informações pelo inimigo ou impedem o reconhecimento de indicadores. Ações como a camuflagem, interferência, desvios, etc, podem ser tomadas para a OPSEC. A terceira categoria consiste na contra-análise. Ela é direcionada ao analista adversário, com a finalidade de que se evite interpretações precisas dos indicadores durante sua análise. Uso de dissimulações são eficientes para se atingir o objetivo (AR 530–1, 2014, p. 24).

A etapa seguinte do gerenciamento do risco em OPSEC é a avaliação do risco. Nessa etapa, a equipe responsável pela elaboração do documento recomenda ao comandante as medidas OPSEC que acreditam que devam ser implementadas, cabendo ao comandante a decisão de efetivá-las. O risco da falha operacional e o custo das medidas adotadas devem ser equilibrados pelo comandante. AR 530–1 (2014, p. 24) também complementa que há preocupação constante com o impacto da medida OPSEC na eficácia operacional e nas futuras missões, além do risco ou impacto se uma medida não for implementada ou não resultar no objetivo proposto.

O *RCC Document 600-11* (2011, p. 2-4) define essa etapa como uma forma de medir o dano ou impacto adverso que uma vulnerabilidade ou a combinação delas pode causar se explorada por um adversário. A avaliação do risco é medida por uma estimativa da capacidade do inimigo em explorar uma vulnerabilidade, os impactos ou efeitos potenciais que tal exploração terá nas operações e, por fim, o levantamento de medidas para controlar a exposição de informações críticas ao inimigo.

A última etapa do gerenciamento de risco preconizada no manual AR 530–1 (2014, p. 25) é a aplicação de medidas e contramedidas de OPSEC. Tem como objetivo a aplicação das medidas aprovadas pelo comandante. São aplicadas nas atividades correntes e nas operações futuras. A equipe designada para OPSEC gera orientações e tarefas para que as medidas sejam cumpridas. Tudo deve ser documentado, incluindo as ações que o comandante julgar que não devam ser executadas.

O MANUAL 5205.02, *DoD Operations Security (OPSEC) Program Manual*, do Departamento de Defesa dos Estados Unidos da América (2020, p. 15), na mesma direção, complementa que, nessa última etapa, as contramedidas devem evitar que a força oponente detecte uma informação crítica ou indicador (dado). Também possui o objetivo de fornecer uma interpretação errônea da informação ou, se possível, negar o acesso a ela.

Ao final do processo, segundo o manual 5205.02 (2020, p. 29), será preenchida a tabela do processo de gerenciamento do risco. Mas antes de se chegar à tabela final, que será abaixo exemplificada, outras tabelas devem ser preenchidas pela equipe OPSEC. Cada tabela corresponde a uma etapa do gerenciamento. Deve-se preencher a tabela de valor das informações críticas, mensurando o impacto que sua perda ou exposição pode acarretar.

A tabela seguinte é a da capacidade de coleta por parte do inimigo. Se ele possui essa habilidade, também deve ser mensurada, quantificando a ameaça. Em seguida, na próxima etapa, deve-se completar a tabela do valor da vulnerabilidade.

Nela são expressos os valores para cada vulnerabilidade de acordo com a probabilidade de exploração da mesma pelo inimigo (5205.02, 2020, p. 28).

5205.02 (2020, p. 29) prossegue que, com os resultados obtidos nas tabelas de ameaça multiplicados pelo valor do nível de vulnerabilidade, é possível obter a probabilidade da perda da informação crítica. Ao final do preenchimento de todas essas tabelas, chega-se à tabela do processo de gerenciamento do risco. A mensuração de todas as tabelas é de alto, médio-alto, médio, médio-baixo e baixo.

Tabela 1 – Processo de gerenciamento do risco OPSEC

<table>
<tr><td colspan="2">INFORMAÇÕES CRÍTICAS</td><td colspan="3" rowspan="2">(Comandante determina qual valor de risco é aceitável para cada vulnerabilidade) Risco aceitável - Médio</td><td colspan="2">AMEAÇA (Analisada em cada disciplina de inteligência)</td></tr>
<tr><td colspan="2">(Informação crítica Nr 1) Nome dos militares empregados na missão</td><td>(Probabilidade da perda da informação crítica) Alta</td><td>SIGINT</td><td>(Valor da ameaça) Alto</td></tr>
<tr><td colspan="2">(Informação crítica Nr 2) Relação de material empregado</td><td>(Probabilidade da perda da informação crítica) Alta</td><td>HUMINT</td><td>(Valor da ameaça) Alto</td></tr>
<tr><td colspan="2">Vulnerabilidade e/ou indicador</td><td>Probabilidade</td><td>Impacto</td><td>Risco</td><td>Contramedidas</td><td>Risco residual</td></tr>
<tr><td>(Vulnerabilidade) Uso de redes de internet sem proteção</td><td>(Valor da vulnerabilidade) Alta</td><td>(Valor da probabilidade) Alta</td><td>(Valor do impacto) Alto</td><td>(Valor do risco) Alto</td><td>(Contramedida a ser adotada) Restringir a coordenação das atividades da missão a redes protegidas. Redução da vulnerabilidade para média</td><td>(Valor do risco) Médio</td></tr>
</table>

Fonte: Manual 5205.02 (2020, p. 29) – Exemplo adaptado pelo autor.

3 PRINCIPAIS SEMELHANÇAS E DIFERENÇAS ENTRE AS DOUTRINAS DO EXÉRCITO BRASILEIRO E DO EXÉRCITO NORTE-AMERICANO

O manual AR 530–1 (2014, p. 7) pontua o comandante, não importando o nível ou escalão, como responsável para desenvolver e implementar um programa de OPSEC no ambiente sob sua responsabilidade. Deve ser uma prioridade em seu comando. Para auxiliá-lo nesta tarefa, será nomeado um oficial coordenador e seu substituto. Tal nomeação deverá ser por escrito e publicada em documento. Os militares devem receber treinamento para ocupar o cargo.

De forma semelhante, o PPCOT (BRASIL, 2020, p. 3-17) sinaliza que o comandante, ciente das ameaças e vulnerabilidades envolvidas na operação, identificará os ativos a serem protegidos. Para tal objetivo, a célula de operações de médio prazo ou seção de planejamento será a responsável direto pela coordenação do gerenciamento de risco na operação.

As OPSEC devem ser contínuas e integradas em todas as operações e atividades militares. AR 530–1 (2014, p. 10) comenta que todos são responsáveis na manutenção da segurança, passando pelo pessoal da ativa, reserva e servidores civis. O principal ativo a ser protegido nas OPSEC é a informação crítica, desde o tempo de paz e planejamento de uma operação.

Da mesma maneira, o Manual EB70-MC-10.307 (BRASIL, 2016, p. 4-2) aponta que atividades de Contrainteligência são de caráter permanente. Devem ser executadas desde o tempo de normalidade, devendo o planejamento de Contrainteligência ser realizado juntamente com os demais planos e ordens de operações. O PPCOT (BRASIL, 2020, p. 3-17) explica que o GRO permite identificar todo tipo de risco associado às operações.

AR 530–1 (2014, p. 2) destaca que que a capacidade de combate está ligada diretamente com a capacidade de obtenção e manutenção da superioridade da informação. Aspectos como levantar, equipar, treinar, desdobrar, dentre outros, são afetados pela informação. O Exército produz informação, portanto, todos devem estar comprometidos com sua segurança, protegendo seus dados. As OPSEC devem ser implementadas na totalidade das Organizações Militares para manter seu sucesso operacional.

Sobre onde o gerenciamento de risco deve ser implementado, EB70-MC-10.307 (BRASIL, 2016, p. 4-3) aborda de forma mais discreta. Cita que o Exame de Situação de Contrainteligência é aplicável a todos os escalões, não sendo detalhista como o manual norte-americano.

EB70-MC-10.220 (BRASIL, 2019c, p. 3-11) possui a definição de segurança que mais se assemelha com uma OPSEC. No que tange à informação, as doutrinas convergem para o objeto de atuação desse grupo de medidas. Atua-se no suporte da informação em si, que são as pessoas, documentos, materiais, os meios de tecnologia da informação e as áreas e instalações.

As etapas do processo de gerenciamento de risco nas OPSEC preconizado pelo manual AR 530–1 (2014, p. 22) são cinco. Elas são voltadas especificamente para a proteção das informações críticas. Nelas, é necessário determinar o que precisa ser protegido, quais recursos o inimigo possui para coletar essas informações, elaborar medidas de OPSEC para se contrapor às ameaças, avaliar os riscos da ação hostil e, por fim, aplicar as medidas planejadas e autorizadas pelo comandante.

É possível observar semelhanças com o prescrito no PPCOT (BRASIL, 2020, p. 3-17) na condução do processo de gerenciamento de risco. Embora o objeto ou ativo a ser protegido não esteja bem definido pelo PPCOT, o GRO permite identificar todo tipo de risco ligado à operação, podendo ser os relacionados às baixas nas tropas amigas, perda ou destruição de equipamentos ou qualquer outro que impacte negativamente na missão.

BRASIL (2020, p. 3-17) divide o GRO em seis etapas. A equipe responsável identifica os fatores de risco ou ameaças, numa primeira etapa sendo seguido, já em outra etapa, pela avaliação do risco, esses dois momentos do gerenciamento se diferem da doutrina norte-americana. A próxima etapa é semelhante à OPSEC que é selecionar medidas para mitigar os riscos. Mais uma semelhança, a etapa de decidir sobre o risco, seguido pela etapa da implementação das medidas aprovadas pelo comandante.

4 CONCLUSÃO

JP 3-13.3 (2016, p. II-1) inicia o capítulo de descrição do processo de OPSEC com uma frase de Maquiavel escrita em seu livro sobre a arte da guerra (1520). “Nenhum procedimento é melhor do que aquele que você escondeu do seu inimigo até o momento que você o executou. Saber reconhecer uma oportunidade na guerra e aproveitá-la beneficia você mais que qualquer outra coisa”.

Portanto, a proteção das informações nas operações militares torna-se uma atividade decisiva para o êxito de uma missão. O GRO, associado ao Exame de Situação de Contrainteligência preenchem essa lacuna de proteção.

Na comparação feita, nota-se relativa concordância nas etapas do processo de gerenciamento. Os processos não se assemelham nas etapas iniciais pois o cerne de cada gerenciamento se difere em sua origem. As OPSEC têm como foco principal a informação crítica e seus indicadores, que seriam os dados isolados da informação. O GRO tem maior amplitude na operação militar, foca nos ativos nela envolvidos.

Da análise da documentação descrita na bibliografia, nota-se a necessidade de revisão doutrinária especificamente na questão de segurança da informação e no próprio processo de avaliação e gerenciamento do risco.

A segurança da informação está inserida no Segmento da Segurança Orgânica, sendo mais um grupo de medidas. Foi observada grande semelhança com as OPSEC que, por força de doutrina, devem ser iniciadas em tempo de paz. A diferença está no objetivo final. As OPSEC devem se estender inclusive para as operações militares, sem interrupções. Já se executa um gerenciamento de risco de OPSEC vislumbrando o emprego da tropa ou Organização Militar em questão. É previsto treinamentos e instruções de OPSEC durante todo o ano.

A avaliação e gerenciamento do risco, na visão do autor, pode sofrer alterações. Tais alterações seriam pontualmente na Matriz de Análise de Gerenciamento de Risco. Volta-se a afirmar que o gerenciamento de risco e OPSEC devem ser realizados o mais cedo possível, durante o planejamento da missão, sendo revisado constantemente para acompanhar as mudanças nas operações correntes e as ameaças decorrentes.

EB70-MC-10.220 (BRASIL, 2019c, p. 2-1), define vulnerabilidade como a deficiência, explorada pela ameaça, que causam eventos não desejados na segurança e geram impactos negativos para o EB. Considerando que a ameaça é o ator motivado e com capacidade de agir, é possível unir a tabela de avaliação de risco com a Matriz de Análise de Risco.

A tabela sugerida vai ao encontro de um dos princípios de guerra: simplicidade. Considera-se que, em operações militares, o tempo para planejamento e execução das operações é um ativo valioso e finito. Quanto mais objetivo for o processo de gerenciamento, não perdendo sua eficiência e eficácia, melhor será para o comandante tomar suas decisões.

Segue sugestão de Matriz Avaliação do Risco e Linhas de Ação:

Tabela 3 – Matriz de Avaliação e tratamento do Risco – Sugestão

Nr Ord	**Vulnerabilidade**	**Probabilidade**	**Impacto**	**Valor do risco**	**Valor do risco aceitável para a vulnerabilidade**	**Tratamento/linha de ação**	**Valor do risco residual**
XX	Descrever, sucintamente, a deficiência e como será explorada	Valor da probabilidade sem tratamento	Valor do impacto sem tratamento	Valor do risco sem tratamento	O Comandante determinará qual será o valor de risco que ele aceita para essa vulnerabilida	Explicar as medidas para tratar o risco e reduzi-lo ao valor determinado pelo comandante	Valor do risco com tratamento

					de		
01	A FT Mec Vermelha pode atacar utilizando apoio aéreo de ARP na região X, a fim de facilitar seu avanço pelo S, uma vez que as tropas que estão na região citada não possuem proteção AAe.	4	2	8	4	O 58º GAAAe colocará uma fração em apoio direto ao 89ª BI Mec, desde já, na região XX, para proteger as tropas na área mencionada.	4

Fonte: O autor.

O valor do risco aceitável será estipulado pelo comandante. Baseado em tabela, aqui não apresentada, pois carece de mais estudo e aprofundamento, a decisão do valor deve ser ponderada com a máxima degradação do poder de combate admitida. A perda de poder de combate será escalonada e expressa em tabela. Por exemplo, se o comandante admite perder, no máximo, 10 % (dez porcento) do poder de combate da fração operacional em estudo, o risco aceitável será considerado “Médio”. Se não for possível aplicar tratamento ao risco e reduzi-lo ao valor determinado pelo comandante, o mesmo deve decidir sobre a continuação da operação ou se o valor aceitável será reavaliado.

É certo que a tabela sugerida necessita de amadurecimento à medida que as operações ou exercícios ocorrerem. A proteção dos ativos e informações críticas é essencial para o cumprimento de uma missão operativa. O uso das OPSEC no Exército norte-americano tem mostrado sua eficácia na proteção dessas informações. Sugere-se estudos mais detalhados sobre tal ferramenta e implantação de medidas de OPSEC também no âmbito EB, impactando positivamente nas medidas de Contrainteligência.

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. Seu horizonte deve ser, ao mesmo tempo, curto para observar os detalhes de uma ameaça, mas longo, para observar o impacto que ocorrerá na Operação caso o inimigo explore uma vulnerabilidade. Apenas com gerenciamento do risco é possível obter essa capacidade de contrapor-se ao oponente, auxiliando o comando na condução de sua missão com sucesso.

REFERÊNCIAS

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

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

BRASIL. Exército Brasileiro. **EB20-D-07-089**: Metodologia da Política de Gestão de Riscos do Exército Brasileiro. 1 ª ed. Brasília, DF, 2017b.

BRASIL. Exército Brasileiro. **EB20-MC-10.202:** Força Terrestre Componente. 1 ª ed. Brasília, DF, 2014a.

BRASIL. Exército Brasileiro. **EB20-MC-10.207:** Inteligência. Brasília, DF, 2015a.

BRASIL. Exército Brasileiro. **EB20-MF-10.102:** Doutrina Militar Terrestre. 1 ª ed. Brasília, DF, 2014b.

BRASIL. Exército Brasileiro. **EB20-MF-10.107**: Inteligência Militar Terrestre. 2 ª ed. Brasília, DF, 2015b.

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

BRASIL. Exército Brasileiro. **EB70-MC-10.211:** Processo de Planejamento e Condução da Operações Terrestres (PPCOT). Brasília, 2ª ed. Brasília, DF, 2020.

BRASIL. Exército Brasileiro. **EB70-MC-10.220:** Contrainteligência. Brasília, 1ª ed. Brasília, DF, 2019c.

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

BRASIL. Exército Brasileiro. **EB70-MC-10.307**: Planejamento e Emprego de Inteligência Militar. 1 ª ed. Brasília, DF, 2016.

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**. MANUAL 5205.02**: *DoD Operations Security (OPSEC) Program Manual*, Departamento de Defesa dos Estados Unidos da América, 2020.

ESTADOS UNIDOS DA AMÉRICA. **NTTP 3-13.3M/MCTP 3-32B**: *Operations Security (OPSEC*), Manual da Marinha dos Estados Unidos da América, Norfolk, VA, 2017.

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

MINISTÉRIO DA DEFESA. Estado-Maior Conjunto das Forças Armadas. **MD30-M-01:** Doutrina de Operações Conjuntas - 2º Volume. 2 ª ed. Brasília, DF, 2020b.

MINISTÉRIO DA DEFESA. Estado-Maior Conjunto das Forças Armadas. **MD30-M-01:** Doutrina de Operações Conjuntas -1º Volume. 2 ª ed. Brasília, DF, 2020a.

RANGE OPERATIONS GROUP OPERATIONS SECURITY COMMITTEE. **Document 600-11**: *Operations Security (OPSEC) Guide*, New Mexico, Estados Unidos da América, 2011.