

**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 (TCC)



**O IMPLEMENTO DA MASINT E O FORTALECIMENTO
DO SISTEMA DE INTELIGÊNCIA DO EXÉRCITO**

**Brasília
2024**

Maj FABIO DOS **SANTOS** MOREIRA

**O IMPLEMENTO DA MASINT E O FORTALECIMENTO
DO SISTEMA DE INTELIGÊNCIA DO EXÉRCITO**

Trabalho de Conclusão de Curso (TCC) 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: MARCELO DO NASCIMENTO **VAILLANT** - TC

**Brasília
2024**

M827i Moreira, Fabio dos Santos

O implemento da MASINT e o fortalecimento do Sistema de Inteligência do Exército/Fabio dos Santos Moreira - 2024.
49 f.

Orientador: Marcelo do Nascimento VAILLANT
Trabalho de Conclusão de Curso (Especialização em Análise de Inteligência)
- Escola de Inteligência Militar do Exército (EsIME), BRASÍLIA/DF, 2024.

1. Inteligência. 2. Inteligência por Assinatura de Alvos. 3. MASINT. 4. Sistema de Inteligência do Exército (SIEx). 5. Exército Brasileiro (EB). 6. Capacidade.

Maj FABIO DOS **SANTOS** MOREIRA

**O IMPLEMENTO DA MASINT E O FORTALECIMENTO
DO SISTEMA DE INTELIGÊNCIA DO EXÉRCITO**

Trabalho de Conclusão de Curso (TCC) 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 2024.

COMISSÃO DE AVALIAÇÃO:

MARCELO DO NASCIMENTO VAILLANT - TC (Presidente)
Escola de Inteligência Militar do Exército

ANDRÉ RICARDO DE OLIVEIRA - Maj (Membro)
Escola de Inteligência Militar do Exército

MARCOS RODRIGO FISCHER PRADO - Maj (Membro)
Escola de Inteligência Militar do Exército

RESUMO

Diante da complexidade que envolve os atuais conflitos e da evolução tecnológica, é necessário que o Exército Brasileiro (EB), por meio do seu Sistema de Inteligência (SIEx) incorpore e explore as mais modernas ferramentas de obtenção e análise de informações e de produção de conhecimentos. Nesse contexto, a Inteligência por Assinatura de Alvos - *Measurement and Signature Intelligence* (MASINT) - surge com uma possibilidade de resposta às exigências do cenário contemporâneo. A MASINT, uma das clássicas Disciplinas de Inteligência, consiste, essencialmente, na captura e medição das características e dos componentes intrínsecos de um alvo, seja ele um objeto ou uma atividade - se algo vibra, se emite um som, se deixa um rastro ou se esquenta ou se esfria, pode emitir uma assinatura explorável e detectável. Como um ramo da Inteligência que se estrutura em atividade científica intensiva, a MASINT disponibiliza aos seus usuários avançados métodos de coleta e análise de dados e informações, que tornam possíveis a identificação e caracterização de algo - um alvo - e a consequente tomada de decisão. A MASINT complementa as tradicionais atividades de inteligência, permitindo compreender de forma mais ampla e precisa o ambiente em que uma crise ou conflito se desenvolve, permitindo ao decisor manter atualizada sua consciência situacional. O emprego da MASINT para fundamentar decisões que vão desde o campo de batalha até as salas de reuniões de chefes de estado é uma tendência global, e a incorporação de suas capacidades ao SIEx representaria o alinhamento deste com os mais avançados sistemas militares de obtenção e processamento de informações do mundo, fortalecendo sua capacidade de apoiar e subsidiar operações militares em cenários que tendem a ser cada vez mais complexos e dinâmicos.

Palavras-chave: Inteligência. Inteligência por Assinatura de Alvos. MASINT. Sistema de Inteligência do Exército (SIEx). Exército Brasileiro (EB). Capacidade.

ABSTRACT

Considering the complexity which involves the current conflicts and the technological advancements, it is imperative for the Brazilian Army, through its Intelligence System, to incorporate and harness the most modern tools for information gathering, analysis, and knowledge production. Within this context, Measurement and Signature Intelligence (MASINT) emerges as a potential response to the demands of the contemporary landscape. MASINT, one of the classical Intelligence Disciplines, essentially involves capturing and measuring the intrinsic characteristics and components of a target, whether it be an object or an activity - if something vibrates, emits sound, leaves a trace, heats up, or cools down, it may emit an exploitable and detectable signature. As a branch of Intelligence structured around intensive scientific activity, MASINT provides its users with advanced methods of data and information collection and analysis, enabling the identification and characterization of a target, and subsequently, decision-making. MASINT complements traditional intelligence activities, allowing a largest and more precise understanding of the environment in which a crisis or conflict unfolds, thus enabling decision-makers to maintain updated situational awareness. The use of MASINT to underpin decisions ranging from the battlefield to state leaders' meeting rooms is a global trend, and the integration of its capabilities into SIEx would align it with the world's most advanced military information gathering and processing systems, enhancing its ability to support and underpin military operations in increasingly complex and dynamic scenarios.

Keywords: Intelligence. Measurement and Signature Intelligence. MASINT. Army Intelligence System. Brazilian Army. Capability.

SUMÁRIO

1 INTRODUÇÃO	9
2 INTELIGÊNCIA POR ASSINATURA DE ALVOS	11
2.1 O QUE É MASINT?	11
2.2 EVOLUÇÃO HISTÓRICA	13
2.3 TIPOS DE MASINT	16
2.3.1 Radar	16
2.3.2 Geofísica	16
2.3.3 Eetro-óptico (EO).....	17
2.3.4 Radiação nuclear.....	17
2.3.5 Radiofrequência (RF)	17
2.3.6 Materiais	18
3 O SISTEMA DE INTELIGÊNCIA DO EXÉRCITO	20
3.1 ONDE SE POSICIONA O SISTEMA DE INTELIGÊNCIA DO EXÉRCITO.....	20
3.2 DOAMEPI.....	20
3.3 O SISTEMA DE INTELIGÊNCIA DO EXÉRCITO E O DOAMEPI.....	21
3.3.1 Doutrina.....	22
3.3.2 Organização (ou processos)	23
3.3.3 Adestramento	24
3.3.4 Material.....	25
3.3.5 Educação	26
3.3.6 Pessoal.....	27
3.3.6 Infraestrutura	27
3.4 CONSIDERAÇÕES FINAIS SOBRE O SIEx - MATRIZ SWOT	28
4 PROPOSTA PARA O IMPLEMENTO DA MASINT NO SIEx	29
4.1 DOCTRINA.....	29
4.1.1 Atualização e integração da doutrina existente	29
4.1.2 Desenvolvimento de normas e procedimentos	29
4.1.3 Normas referentes à capacitação e ao treinamento.....	30
4.1.4 Documentação e manuais operacionais	30
4.1.5 Interoperabilidade Doutrinária	30
4.2 ORGANIZAÇÃO.....	31
4.2.1 Estruturação de equipes, frações ou módulos especializados	31

4.2.2 Integração com outras Disciplinas de Inteligência	31
4.2.3 Expansão geográfica	31
4.2.4 Cargos e carreiras	31
4.2.5 Estrutura de apoio	32
4.3 ADESTRAMENTO	32
4.3.1 Programas de Adestramento Avançado (PAA)	32
4.3.2 Treinamento prático e simulações.....	32
4.3.3 Certificação e qualificação	33
4.3.4 Parcerias educacionais como oportunidades de adestramento.....	33
4.3.5 Adestramento em segurança cibernética	33
4.4 MATERIAL	34
4.4.1 Investimento em tecnologia avançada	34
4.4.2 Atualização de infraestrutura	34
4.4.3 Parcerias Público-Privadas	34
4.4.4 Segurança da informação.....	35
4.4.5 Integração de sistemas.....	35
4.5 EDUCAÇÃO	36
4.5.1 Currículos voltados para MASINT	36
4.5.2 Programas de pós-graduação e especialização.....	36
4.5.3 <i>Workshops</i> e seminários	36
4.5.4 Educação continuada	36
4.5.5 Pesquisas e publicações	37
4.6 PESSOAL.....	37
4.6.1 Seleção.....	37
4.6.2 Retenção de talentos	37
4.6.3 Capacitação contínua	38
4.7 INFRAESTRUTURA.....	38
4.7.1 Desenvolvimento de instalações especializadas	38
4.7.2 Manutenção e atualização de infraestruturas.....	38
4.7.3 Segurança física e tecnológica	39
4.7.4 Investimento em tecnologias emergentes	39
4.7.5 Parcerias para o desenvolvimento de tecnologias e infraestruturas	39
5 CONCLUSÃO	40
REFERÊNCIAS.....	43

APÊNDICE A - Análise do SIEx empregando a Matriz <i>SWOT</i>.....	45
1 PONTOS FORTES	45
2 OPORTUNIDADES.....	46
3 PONTOS FRACOS.....	47
4 AMEAÇAS	48

1 INTRODUÇÃO

O cenário atual é marcado por intenso agito e significativas transformações geopolíticas que exigem evolução constante nas estratégias de segurança e defesa.

O mundo vive **desafios mais complexos** do que os enfrentados durante o período passado de confrontação ideológica bipolar. O fim da Guerra Fria reduziu o grau de previsibilidade das relações internacionais que estavam vigentes desde a 2ª Guerra Mundial (Brasil, 2005, grifo próprio).

Nesse ambiente, reduziu-se significativamente a possibilidade de um conflito generalizado entre Estados. Porém, ganharam nova impulsão os conflitos de caráter étnico e religioso, de exacerbação de nacionalismos e a fragmentação de Estados, com uma amplitude e ressonância que ameaçam a ordem mundial (Brasil, 2005).

As novas ameaças exigem que os Estados estejam aptos para o combate ao terrorismo; proteção contra armas de destruição em massa; participação em missões de manutenção e/ou de imposição da paz sob a égide de organismos internacionais; oferecimento de ajuda em caso de catástrofes; e controle de massas populacionais ou de recursos escassos como energia, água ou alimentos (Brasil, 2022).

Como integrante desse sistema de defesa e segurança, as Forças Armadas - constituídas também pelo Exército Brasileiro (EB), do qual deriva a Força Terrestre (F Ter) - precisam se adaptar às transformações em curso.

A Doutrina Militar Terrestre (DMT) deve ser permanentemente atualizada em função da evolução da natureza dos conflitos, do resultado das mudanças da sociedade e da evolução tecnológica. (...) As mudanças experimentadas pelas sociedades, com reflexos na forma de fazer política e o surgimento de nova configuração geopolítica, conduzem a horizontes mais incertos e complexos para planejar a Defesa da Pátria (Brasil, 2022).

As mudanças inevitavelmente refletirão nos elementos do Poder de Combate Terrestre, que representam a essência das capacidades que a F Ter utiliza quando empregada. Os elementos são: Liderança, Informações e as Funções de Combate - dentre elas, a Função de Combate Inteligência (Brasil, 2022a).

Prover inteligência eficaz está se tornando mais desafiador à medida que as operações se tornam mais complicadas. O atual ambiente é dinâmico, complexo e moldado pela interseção de tendências globais impulsionadas pela globalização, novas tecnologias, mudanças climáticas e diferentes estágios de conflito e resolução destes (Estados Unidos da América, 2023).

¹ Oficial de Infantaria do Exército Brasileiro - Academia Militar das Agulhas Negras. Pós-graduado em Ciências Militares - Escola de Comando e Estado-Maior do Exército.

No Exército Brasileiro, a execução das atividades e tarefas de inteligência ou os processos ligados à sua regulamentação e normatização estão sob a égide do Sistema de Inteligência do Exército (SIEx) (Brasil, 2015a).

Nesse cenário em que a evolução tecnológica desempenha papel crucial, oferecendo oportunidades e exigindo a incorporação de novas capacidades, surge para o SIEx o dever de considerar as tendências e as ferramentas que irrompem a todo instante na chamada Comunidade de Inteligência.

Assim, a MASINT - *Measurement and Signature Intelligence* - ou Inteligência por Assinatura de Alvos, uma das Disciplinas de Inteligência - cujas características a colocam como intensiva em tecnologia e que requer pessoal versado em uma vasta gama de ciências físicas e elétricas (EUA, 1996) - coloca-se como um campo para a aquisição de aptidões que permitirão o incremento de novas possibilidades no SIEx.

A MASINT, com seus métodos avançados de coleta e análise de informações, complementa e aprimora a atividade de Inteligência. Assim, ante a constatação de que o SIEx não explora as capacidades relacionadas à MASINT, a realização deste estudo se justifica, uma vez que seus objetivos são destacar a importância da adoção dessa disciplina de Inteligência, promover a disseminação e o conhecimento do assunto e fomentar o estudo e o desenvolvimento de doutrina nessa área.

De maneira a facilitar a compreensão, o primeiro capítulo apresentará o tema MASINT - suas definições, evolução histórica e principais tipos - visando permitir que se conheça, mesmo que em um nível básico, o assunto central.

O segundo capítulo tratará sobre o SIEx de acordo com os sete fatores determinantes e indissociáveis da Capacidade Operativa - Doutrina, Organização, Adestramento, Material, Educação, Pessoal e Infraestrutura (DOAMEPI) (Brasil, 2022a) - visa-se adquirir a percepção de que a MASINT não é explorada pelo Sistema de Inteligência do Exército em sua plenitude.

Por sua vez, o último capítulo, ainda considerando os fatores representados pelo acrônimo DOAMEPI, apresentará as oportunidades de inserção da MASINT no SIEx, de maneira a fortalecê-lo e permitir o aumento de sua amplitude.

O trabalho pretende não somente apresentar uma forma de fortalecer o SIEx, como também destacar a urgência do desenvolvimento de capacidades tecnológicas próprias e adaptadas às necessidades das operações militares contemporâneas.

2 INTELIGÊNCIA POR ASSINATURA DE ALVOS

De acordo com a Doutrina Militar Terrestre atual, a Inteligência por Assinatura de Alvos - *Measurement and Signature Intelligence* (MASINT) - é uma das nove disciplinas clássicas de inteligência (Brasil, 2015a).

Segundo a doutrina militar nacional, uma disciplina de Inteligência concentra em si os diferentes recursos, meios, sistemas e técnicas utilizados para observar, explorar armazenar e difundir as informações de uma determinada situação, ameaça ou outro aspecto presente no ambiente operacional (Brasil, 2015a).

Por sua vez, a doutrina militar norte-americana informa que uma disciplina de Inteligência se caracteriza como um campo bem definida de planejamento na área de inteligência, coleta, exploração, análise e produção de relatórios por meio do uso de uma categoria específica de recursos técnicos ou humanos (EUA, 2023).

2.1 O QUE É MASINT?

Para facilitar o entendimento sobre um termo pouco conhecido, ressalta-se o breve relato de um fato verídico ocorrido nos primeiros meses do ano de 2023:

Em 3 de abril de 2023, a rede NBC News confirmou através de fontes oficiais americanas que a República Popular da China, por meio de um balão que sobrevoou os céus dos Estados Unidos da América, **havia coletado e transmitido sinais de dados provenientes de sistemas de armas americanos**. Os sinais emanados poderiam revelar a posição ou quantidade de mísseis localizados em uma base específica. Eles poderiam até determinar a presença de ogivas nucleares (Singh, 2023, tradução nossa, grifo próprio).

Segundo o Gabinete do Diretor de Inteligência Nacional dos Estados Unidos da América - *Office of the Director of National Intelligence* - MASINT é uma disciplina de Inteligência baseada na captura e na medição das características e componentes intrínsecos de um alvo - objeto ou atividade - permitindo sua detecção, identificação e caracterização. Caso o alvo vibre, emita um som, deixe um rastro ou esquente ou esfrie, pode emitir uma assinatura explorável (Estados Unidos da América, 2022).

Tem-se que no termo - *Measurement and Signature Intelligence* - a palavra “*measurement*” - medição² - se refere a qualquer informação obtida e gravada durante a coleta pelos diversos sensores empregados em MASINT (Lowenthal; Clark, 2015).

² Tradução nossa.

Estes sensores têm a finalidade de identificar as características associadas à origem - ou alvo - que podem ser classificadas como nucleares, químicas, biológicas, térmicas, eletromagnéticas, sonoras e dinâmicas, dentre outras (Seng, 2007).

A informação, após a remoção do conteúdo indesejado - não pertencente ao alvo, como ruídos atmosféricos, por exemplo - é colocada em um formato padrão, definindo assim sua “*signature*” - assinatura³.

Formada a primeira assinatura, é possível utilizá-la como um parâmetro para comparar dados de coletas futuras, permitindo identificar um alvo. A repetição do processo, aliada a outras fontes para confirmação permite a atualização da assinatura original (Lowenthal; Clark, 2015).

Como exemplo, tem-se o seguinte: múltiplos sensores captam perturbações sonoras, sísmicas e térmicas. Comparando-se as leituras obtidas com os parâmetros já conhecidos e catalogados, verifica-se que o som é correspondente ao ruído de turbinas, que os tremores possuem intensidade compatível aos de decolagem de uma aeronave e que sua origem aponta para um local onde há uma pista de pouso e decolagem e, por fim, que as emissões térmicas coincidem com o calor produzido por turbinas de um determinado modelo. Assim, tem-se a conclusão de que se trata da decolagem de uma aeronave de asa fixa de alta performance - um caça (Seng, 2007).

Conforme expressaram Lowenthal e Clark (2015), MASINT é uma disciplina de Inteligência de natureza iminentemente técnica que permite detectar, localizar, rastrear, identificar e descrever características únicas de fontes fixas ou dinâmicas.

De acordo com a Doutrina Militar Terrestre, é a inteligência proveniente da análise científica e técnica de dados obtidos de fontes emissoras com o propósito de identificar as características associadas a essas fontes, facilitando sua identificação. Suas formas de obtenção podem sobrepujar a maioria das técnicas de camuflagem, ocultação e dissimulação que são utilizadas na atualidade e, por meio de uma análise e difusão em tempo próximo ao real, pode proporcionar uma visão da situação que não poderia ser obtida por outras disciplinas de inteligência (Brasil, 2015a).

Novamente de acordo com Lowenthal e Clark (2015), a obtenção de dados utilizados na MASINT inclui o uso de sensores especializados, tais como radares de vigilância, espectrômetros eletromagnéticos e sensores de infravermelho, que podem detectar assinaturas únicas como, por exemplo, emissões de calor, padrões de ondas

³ Tradução nossa.

eletromagnéticas e características espectrais. Esses dados, por sua vez, são associados a alvos ou complementam outras disciplinas de inteligência, fornecendo percepções adicionais sobre um determinado objeto, local ou atividade de interesse, permitindo, inclusive, a identificação de ameaças ocultas a outros meios de detecção.

Os meios MASINT têm capacidades únicas para detectar o lançamento de mísseis, identificar e seguir plataformas aéreas, embarcações e veículos em geral, colaborar com a avaliação dos efeitos do combate e detectar e monitorar a ocorrência de chuva radioativa provocada por armamento nuclear (Brasil, 2015a).

A MASINT é uma disciplina intensiva em ciência que necessita de pessoas com experiência em pesquisa e desenvolvimento e de profissionais das diversas áreas do conhecimento, como física e elétrica (Estados Unidos da América, 2016)

Assim, a Inteligência por Assinatura de Alvos se dedica à detecção e análise de padrões de energia, de materiais e de processos associados a alvos específicos que emitem essas assinaturas. A MASINT pode complementar outras disciplinas de inteligência ao fornecer informações que não podem ser obtidas por meio de métodos convencionais, sendo essencial para identificar alvos que foram ocultados e apoiando a tomada de decisões em operações militares e de segurança nacional.

2.2 EVOLUÇÃO HISTÓRICA

Para facilitar o entendimento sobre o emprego de uma capacidade tão pouco conhecida, destaca-se o breve resumo cronológico de fatos verídicos ocorridos em duas décadas específicas do século XX:

Agosto de 1949 - a União das Repúblicas Socialistas Soviéticas (URSS) detona sua bomba atômica. É o início da Guerra Fria. **Novembro de 1955** - os soviéticos testaram a bomba de hidrogênio, cuja entrega é mais adequada por míssil. **Agosto de 1957** - a URSS realiza o primeiro teste bem-sucedido de um míssil balístico intercontinental. **Outubro de 1957** - os soviéticos orbitaram com sucesso o satélite artificial Sputnik 1 - É dada a largada para a Corrida Espacial começou (Morris, 2019, tradução nossa, grifo próprio).

A detecção de um som subaquático para identificar submarinos submersos e o uso de sensores acústicos para localizar a artilharia de campanha inimiga datam da Primeira Grande Guerra. A utilização de radar para detectar, identificar, e rastrear aeronaves e navios surgiu durante a Segunda Guerra Mundial (II GM) e, ao longo desse conflito, detectores químicos surgiram ante o emprego de armas dessa natureza e foram amplamente utilizados (Lowenthal; Clark, 2015).

Os autores deixam evidente que, pouco depois da II GM, as técnicas que hoje são consideradas MASINT eram exclusivamente aplicadas para apoiar operações militares - nível tático - e não eram estruturadas como uma disciplina de Inteligência.

Contudo, esse quadro muda devido ao início dos testes nucleares soviéticos. Segundo Lowenthal e Clark (2015), a MASINT passou a ter importância estratégica, uma vez que os Estados Unidos de América precisavam dimensionar - com elevado grau de precisão - as capacidades nucleares adquiridas pela antiga URSS.

Morris (2019) diz que, já no final da década de 1950, sistemas de vigilância sísmica e sonora - *Seismic and Sound Surveillance System (SOSUS)* - estavam em funcionamento e radares de feixe fixo eram implantados para a vigilância de mísseis.

Ao longo da década de 1960, expandiu-se a rede SOSUS, voos para coleta de amostras do ar se tornaram rotina, foi feita a detecção de míssil vindo do espaço por meio do uso de dispositivos de infravermelho e radares de rastreamento de feixe único de precisão foram implantados. No fim dessa década, aeronaves de vigilância RC-135 estavam plenamente operacionais e navios de instrumentação de alcance avançado - *Advanced Range Instrumentation Ships (ARIS)* - utilizando radares de rastreamento de feixe único foram implantados.

Lowenthal e Clark (2015) informam que sensores acústicos e sísmicos foram pela primeira vez utilizados pelos Estados Unidos da América no final da década de 1960, durante a Guerra do Vietnã, para monitorar a infiltração de soldados inimigos e suprimentos que entravam no Vietnã do Sul ao longo da "Trilha Ho Chi Minh".

Morris (2019) ressalta que, no início da década de 1970, a Força Aérea dos EUA lançou o primeiro satélite operacional de alerta precoce do Programa de Apoio à Defesa - *Defense Support Program (DSP)* - sistematizaram-se as assinaturas de mísseis e outros perfis que passaram a ser usados na classificação de ameaças e de alvos diversos e radares de imagem de longo alcance foram desenvolvidos para a identificação de objetos espaciais.

A Agência de Inteligência de Defesa - *Defense Intelligence Agency (DIA)* - a Agência de Inteligência Central - *Central Intelligence Agency (CIA)* - e a Força Aérea dos EUA estabeleceram inteligências baseadas em radar e em instrumentos ópticos - RADINT e OPTINT. Em 1974, o Diretor da CIA, principal conselheiro do Presidente norte-americano e do Conselho de Segurança Nacional para questões de inteligência estrangeira, determinou a criação dos comitês SIGINT, IMINT e HUMINT para que fossem estabelecidos os requisitos de obtenção de dados por meio de sinais, de

imagens e de fontes humanas, respectivamente. Em paralelo, o termo Inteligência de Medição e Assinatura - *Measurement and Signature Intelligence* (MASINT) - foi, pela primeira vez, usado pela Agência de Inteligência de Defesa dos EUA (Morris, 2019).

A Guerra Fria, de 1947 a 1991, fomentou sobremaneira o desenvolvimento da MASINT e a consolidou como imprescindível. Tanto os EUA quanto a antiga URSS implementaram rigorosas medidas de segurança em seus respectivos territórios, dificultando a obtenção de dados e conhecimentos através de fontes humanas, sinais ou imagens. Diante das restrições, os recursos e meios das tecnologias de detecção de assinaturas e medição relacionadas à MASINT contornaram tais obstáculos, fornecendo informações precisas sobre as armas e os testes nucleares realizados pelos soviéticos. À medida que sua importância estratégica da MASINT crescia, diminuía a frequência do seu uso em operações militares (Lowenthal; Clark, 2015).

No entanto, não apenas a questão nuclear fortaleceu a MASINT. Um outro episódio histórico também o fez: “A Corrida Espacial entre EUA e URSS”. Lowenthal e Clark (2015) dizem que os novos métodos analíticos e tecnologias impulsionaram aquilo que pode ser considerado como a terceira grande onda de desenvolvimento da MASINT. As aplicações táticas e a questão nuclear - armamento estratégico - são as duas primeiras.

Segundo os autores, já em 1986, a MASINT, consolidada entre os membros e as agências da comunidade de inteligência norte-americana, ensejou a criação de um comitê dedicado a conduzir políticas em sua área de atuação para o desenvolvimento de novas capacidades. No ano de 1992, o sucesso da comissão fez com que fosse criado o Escritório Central de MASINT - *Central MASINT Office* (CMO).

Nas últimas duas décadas, como consequência das inovações tecnológicas e da supervisão a nível nacional desempenhada pelo CMO, a MASINT experimenta sua quarta grande onda de desenvolvimento e aplicação e retorna às suas origens, no campo de batalha. Novos níveis de experiência analítica aliados a computadores mais potentes, extensas e ágeis redes de comunicação, novos sensores, tecnologias de processamento e exploração baseadas em assinaturas e diversas plataformas de coleta se uniram para possibilitar a entrega - em tempo real - de uma variedade de produtos para as unidades de combate. Como resultado, a MASINT se torna parte importante para as operações militares, fazendo-se presente em aplicações como previsão do tempo, planejamento e execução de operações diversas, mapeamento do terreno, avaliação de danos e emissão de alertas (Lowenthal; Clark, 2015).

2.3 TIPOS DE MASINT

De acordo com Singh (2023) e com o Escritório do Diretor de Inteligência Nacional⁴, a MASINT possui seis tipos, que, conforme destaca Richelson (2001), existiam antes mesmo de essa se tornar uma disciplina de Inteligência reconhecida.

2.3.1 Radar

A MASINT baseada em radares emprega um sistema no qual é possível obter informações de um objeto por meio de pulsos de ondas de alta frequência que são refletidas no alvo e que retornam à fonte, permitindo sua análise e a obtenção de informações (EUA, 2022).

No nível macro, o radar pode fornecer assinaturas de localização, velocidade e aceleração que permitem avaliar o desempenho de mísseis e aeronaves. No nível micro, podem obter a configuração e a composição de alvos e ainda gerar imagens de corpos como aeronaves, ogivas de mísseis e satélites (Lowenthal; Clark, 2015).

Neste caso, radares são usados para analisar e medir características, em vez de coletar informações diretas como é feito em inteligência de sinais (Singh, 2023).

2.3.2 Geofísica

Esse tipo de MASINT é baseada nos fenômenos físicos da Terra - eventos de energia e distúrbios que afetam a ionosfera, a atmosfera, os oceanos, a litosfera e até regiões abaixo da crosta terrestre (EUA, 2022).

Explorando tanto as frequências audíveis quanto as inaudíveis, pode-se, por exemplo, detectar vibrações de máquinas em operação, explosões subterrâneas, ou mesmo diferenças de pressão criadas pela abertura e fechamento das portas dos silos das instalações de lançamento de mísseis (Lowenthal; Clark, 2015).

Esta forma de MASINT auxilia na compreensão de informações vitais por meio da detecção de assinaturas de plataformas submarinas ameaçadoras e das daquelas provenientes da operação de sistemas de mísseis balísticos lançados por submarinos e de outras armas lançadas no mar. Operacionalmente, contribui para a detecção, classificação e vigilância de mísseis, submarinos, navios, veículos e aeronaves, podendo, ainda, ser útil na avaliação de ameaças (EUA, 2022).

4 Office of the Director of National Intelligence, Estados Unidos da América, 2022.

2.3.3 Eletro-óptico (EO)

De acordo com o Escritório Central de MASINT norte-americano (EUA, 2022), a EO MASINT se baseia na coleta de energia na porção óptica - ultravioleta, luz visível, infravermelho próximo e infravermelho - do espectro eletromagnético.

Os dados são coletados por uma variedade de dispositivos ópticos sensíveis - radiômetros, espectrômetros, sistemas não-imagem, lasers, fibras ópticas e outros - que podem ser usados para rastrear e caracterizar veículos de reentrada voando em testes de voo de mísseis balísticos e detonações nucleares, por exemplo.

2.3.4 Radiação nuclear

Caracterizada pela detecção, coleta e medição ativa ou passiva de raios gama, nêutrons, raios X ou de outros fenômenos de radiação de fontes nucleares.

Os sensores incluem dispositivos a bordo de aviões ou de satélites, sensores portáteis usados por agentes alfandegários e outros que detectam e identificam a transferência de materiais nucleares. Materiais-alvo incluem isótopos de urânio e plutônio - usados em armas nucleares - e materiais radioativos como raios gama

A detonação da primeira bomba atômica por parte da URSS, em 1949, despertou nos EUA a necessidade de se desenvolver um método para detectar testes de armas nucleares em todo o mundo (EUA, 2022).

2.3.5 Radiofrequência (RF)

Incluem pulsos eletromagnéticos nucleares - verdadeiros ou simulados - além de sinais intencionalmente irradiados ou colateralmente advindos em consequência de emissões irradiadas involuntariamente por fontes mecânicas e eletrônicas ou do uso de armas de frequência de rádio (RFW)⁵ (EUA, 2022).

Em 2016, funcionários da embaixada dos EUA em HAVANA, Cuba, informaram dores de cabeça, dificuldades cognitivas e de equilíbrio, normalmente associadas a traumas na cabeça. Eles informaram ter ouvido um intenso barulho. Em 2018, houve um fato similar na China, quando funcionários da embaixada dos EUA apresentaram

⁵ Os sistemas de armas de frequência de rádio - *Radio Frequency Weapons* (RFW) - usam energia eletromagnética para desativar sistemas eletrônicos. Eles produzem pulsos eletromagnéticos curtos, intensos e direcionados que perturbam ou danificam alvos eletrônicos. Dentre suas capacidades, inclui-se a de poder danificar uma grande variedade de componentes, como os encontrados em aeronaves, munições, satélites, sistemas de defesa aérea ou em equipamentos de C², comunicações, computação, inteligência, vigilância e reconhecimento (EUA, 2022).

os sintomas observados em 2016. As evidências indicaram o uso de um dispositivo de micro-ondas que afetou a estrutura neural das pessoas (Canham, 2019).

Essa subdisciplina se baseia nas emissões rádio, intencionais ou não, como as oriundas de motores, sistemas de armas, sistemas eletrônicos, equipamentos e instrumentos, com o objetivo de encontrar assinaturas que possam identificar um alvo.

Por meio dos sinais de radiofrequência, é possível determinar, por exemplo, se um equipamento está ligado ou não. Motores de blindados e de caminhões emitem energia eletromagnética por meio das velas de ignição, assim essa energia pode ser captada e comparada, permitindo a identificação do veículo (Lowenthal; Clark, 2015).

A RF MASINT pode ser usada para detectar, localizar, identificar, caracterizar e visar ameaças, ao diagnosticar os parâmetros técnicos de um alvo, determinando seus níveis de potência, características operacionais e assinaturas.

Os resultados da exploração de RF MASINT sobre sistemas de armas de RF permitem o desenvolvimento ou o uso de contramedidas e fornecem avaliações das tecnologias avançadas de armas empregadas pelos adversários (EUA, 2022).

2.3.6 Materiais

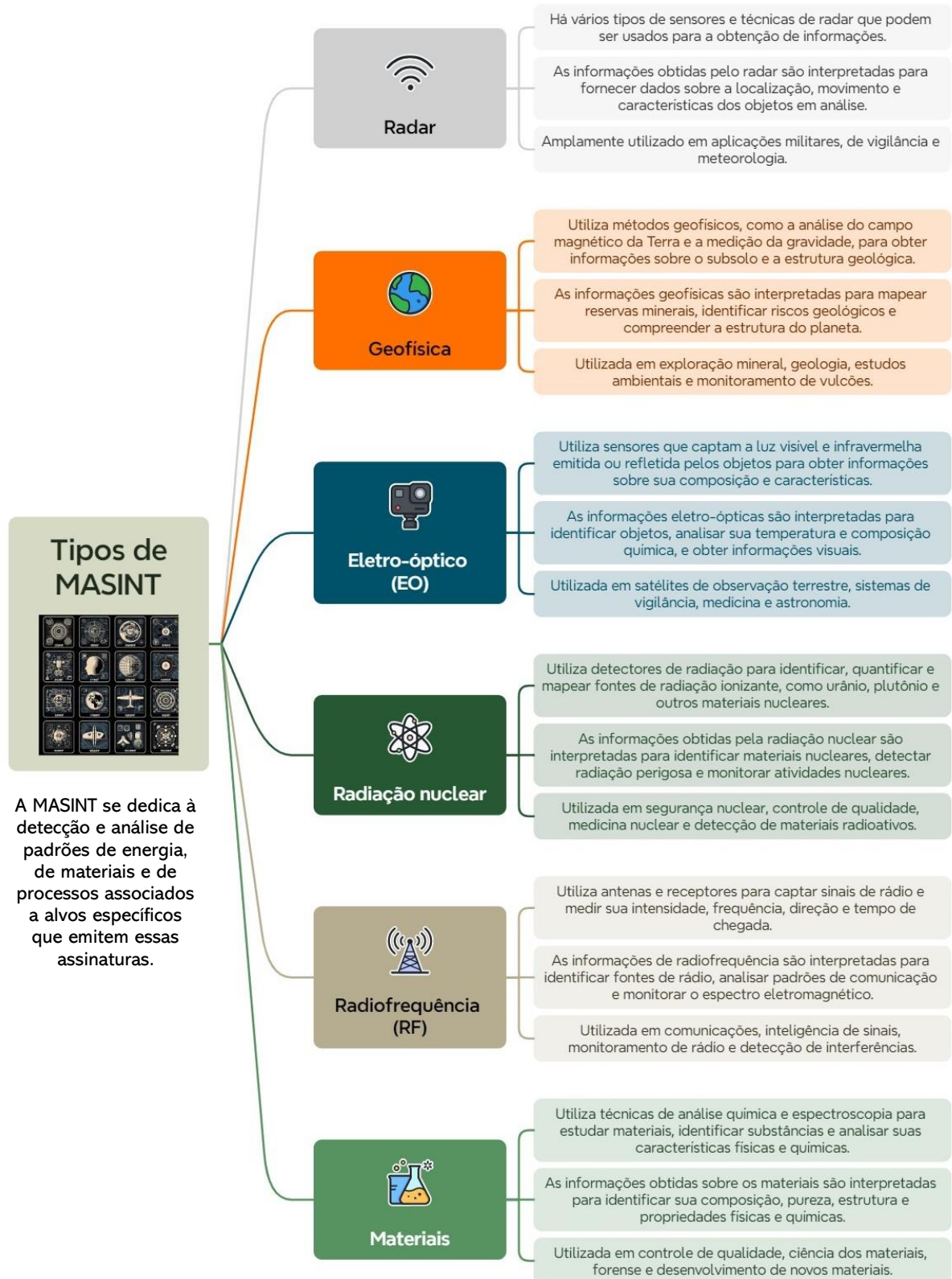
Esse tipo de MASINT é baseado na coleta de amostras de material sólido, ar ou água de um determinado local-alvo ou próximo a ele, que são analisadas com o objetivo de se encontrar - ou não - assinaturas isotópicas, químicas ou biológicas.

As amostras são utilizadas para a determinação de assinaturas isotópicas, químicas ou biológicas. No caso de materiais avançados, essa subdisciplina explora cerâmicas, compósitos, orgânicos, materiais metálicos, materiais inteligentes e materiais especiais para aplicações em blindagens, armas e veículos.

Ainda, as amostras são analisadas segundo o seu potencial para aplicações nas áreas de energia, clínica ou biomédica. Agentes materiais apresentam desafios únicos para análises confirmatórias e para a atribuição conclusiva quanto à sua origem quando encontrados no ambiente (EUA, 2022).

Muitos países desenvolveram sensores e metodologias para detecção pontual e à distância de materiais químicos, biológicos, radiológicos, nucleares e explosivos (CBRNE). A possibilidade de que esses materiais possam ser usados em ataques terroristas tem impulsionado esse desenvolvimento. Além disso, tratados que limitam a produção, uso e a proliferação de tais materiais têm exigido o estabelecimento de regimes internacionais de monitoramento (Lowenthal; Clark, 2015).

Figura 1 - Tipos de MASINT



Fonte: Compilação do autor⁶.

⁶ Compilação feita a partir das diversas obras utilizadas como fonte de consulta para a elaboração deste trabalho.

3 O SISTEMA DE INTELIGÊNCIA DO EXÉRCITO

3.1 ONDE SE POSICIONA O SISTEMA DE INTELIGÊNCIA DO EXÉRCITO

A atual Política Nacional de Inteligência foi fixada pelo Decreto Nr 8.793, de 29 de junho de 2016, e tem a finalidade de definir os parâmetros e os limites de atuação da atividade de Inteligência e de seus executores, além de estabelecer os pressupostos, objetivos, instrumentos e diretrizes, no âmbito do Sistema Brasileiro de Inteligência (SISBIN) (Brasil, 2016).

Anteriormente ao decreto citado acima, o SISBIN foi instituído pela Lei Nr 9.883, de 7 de dezembro de 1999, com o objetivo de integrar as ações de planejamento e de execução das atividades de inteligência do país e fornecer subsídios ao Presidente da República nos assuntos de interesse nacional (Brasil, 1999).

A mais recente alteração do SISBIN - Decreto Nr 11.693, de 6 de setembro de 2023 - estabelece que, como um de seus órgãos permanentes, com competências relativas à governabilidade, à segurança interna, à defesa e às relações externas do país, encontra-se o Centro de Inteligência do Exército (CIE) do Comando do Exército do Ministério da Defesa (Brasil, 2023a).

Conforme o manual de fundamentos EB20-MF-10.107 - Inteligência Militar Terrestre (Brasil, 2015a, grifo próprio), o CIE tem a incumbência de ser o órgão central do Sistema de Inteligência do Exército, proporcionando a estrutura para o devido fluxo de conhecimento e para o gerenciamento do próprio sistema.

Assim, tem-se o ponto de interseção pelo qual fica, formalmente estabelecida, a ligação entre a Política Nacional de Inteligência (PNI) e o Sistema de Inteligência do Exército, além do seu respectivo posicionamento - do SIEx - na organização do SISBIN, estrutura responsável pela execução da Política Nacional de Inteligência.

3.2 DOAMEPI

O Exército Brasileiro adota a geração de forças por meio do Planejamento Baseado em Capacidades (PBC). Por sua vez, capacidade é a aptidão necessária a uma força ou organização militar para o cumprimento de determinadas missões ou atividades. Essa aptidão será exercida sob condições e padrões determinados, pela combinação de meios para desempenhar uma gama de tarefas.

Ainda, de maneira sistêmica, obtém-se a capacidade a partir de um conjunto de sete fatores determinantes, relacionados e indissociáveis entre si: Doutrina, Organização, Adestramento, Material, Educação, Pessoal e Infraestrutura, os quais formam o acrônimo DOAMEPI (Brasil, 2022a).

3.3 O SISTEMA DE INTELIGÊNCIA DO EXÉRCITO E O DOAMEPI

Antes de apresentar os aspectos do SIEx atinentes a cada item do DOAMEPI, ressalta-se que os fatores não podem ser vistos isoladamente. Assim, uma mesma característica ou conceito do SIEx - a partir da compreensão daquilo que representa cada fator determinante - pode se relacionar com mais de um dos sete atributos que caracterizam uma capacidade.

Ainda, diante da relevância do Programa Estratégico do Exército LUCERNA (Prg EE LUCERNA), optou-se por apresentar suas contribuições para o incremento de capacidades ao SIEx em cada um dos subitens a seguir. A iniciativa reforçou as capacidades já existentes, tornando-as mais efetivas e trouxe novas possibilidades sem suplantando e substituir os fatores que já caracterizavam o SIEx, contribuindo para a robustez do sistema e fomentando o seu fortalecimento.

O Prg EE LUCERNA teve sua Diretriz de Iniciação aprovada no ano de 2017. Seu objetivo-síntese é readequar o SIEx em função das demandas atuais e futuras e da disponibilidade de recursos. Essa diretriz determinou que o Estudo de Viabilidade (EV) do programa estivesse alinhado com a Concepção Estratégica do Exército e com o Plano Estratégico do Exército (PEEx), bem como incorporasse estudos e conclusões, segundo o acrônimo DOAMEPI (Brasil, 2017).

Em 2020, foi aprovada a Diretriz de Implantação do Prg EE LUCERNA - EB20-D-08.040 - para transformar o SIEx, aumentando sua capacidade de obter dados, por meio da adaptação e/ou criação de entes ou Organizações Militares voltados para a Inteligência de Combate, e expandindo o seu poder de análise (Brasil, 2020).

Para o atingimento de tal objetivo, a diretriz em questão estabeleceu que o Prg EE LUCERNA enquadraria três projetos:

- Projeto ATENA, voltado para a atualização e a modernização do ensino da Disciplina Inteligência Militar (IM) no âmbito do EB;
- Projeto HERMES, focado na modernização da estrutura de Tecnologia da Informação e Comunicações (TIC); e

- Projeto ARES, direcionado para a transformação - gradual e faseada - das atuais estruturas de Inteligência Militar distribuídas nos diversos escalões da F Ter.

A seguir, considerando os aspectos e condições acima, são apresentados os fatores determinantes que caracterizam o Sistema de Inteligência do Exército:

3.3.1 Doutrina

Conjunto de princípios, conceitos, normas e procedimentos que necessitam ser organizados e expostos de forma integrada e harmônica, cuja fundamentação se sustenta principalmente na experiência, e que tem por objetivo estabelecer linhas de pensamentos e orientar ações (Brasil, 2015b).

Base para os demais fatores determinantes, é materializada nos produtos doutrinários que delineiam um ente - o SIEx, no caso específico (Brasil, 2022a).

Com observância desse quadro, o manual de fundamentos EB20-MF-10.107 - Inteligência Militar Terrestre (Brasil, 2015a) dedica o seu capítulo VII a apresentar e a conceituar o SIEx.

Ainda, é possível verificar um conjunto de produtos doutrinários cujo objetivo é normatizar aspectos e outros fatores determinantes do SIEx. Ao se consultar a Relação de Publicações do Exército - REPUBLEx (Brasil, 2024), encontra-se:

- EB20-MC-10.207 - Inteligência;
- EB70-MC-10.220 - Contraineligência;
- EB70-MC-10.252 - Inteligência nas Operações;
- EB70-MC-10.302 - Batalhão de Inteligência Militar;
- EB70-MC-10.307 - Planejamento e Emprego da Inteligência Militar;
- EB70-MC-10.312 - Companhia de Inteligência Militar;
- EB70-MC-10.322 - Inteligência de Sinais;
- EB20-MF-10.107 - Inteligência Militar Terrestre;
- EB70-MT-10.401 - Produção do Conhecimento de Inteligência;
- EB70-MT-70.402 - Geointeligência; e
- EB70-CI-11.465 - TTP da Tropa Como Sensor de Inteligência.

Somam-se a esses produtos doutrinários, os já previstos para elaboração ou difusão no Plano de Desenvolvimento da Doutrina Militar Terrestre (PDDMT)/2024 (Brasil, 2023b), conforme a seguir:

- EB70-MC-10.XXX - Inteligência de Fontes Humanas;

- EB70-MC-10.XXX - Geointeligência - atual EB70-MT-10.402;
- EB70-MC-10.2XX - Contraineligência nas Operações;
- EB70-MC-10.356 - Inteligência Cibernética;
- EB70-CI-11.XXX - TTP de Rec e Vig de Inteligência Militar;
- EB70-MT-10.XXX - Inteligência de Fontes Abertas;
- EB70-MT-10.XXX - Inteligência de Saúde;
- EB70-MT-10.4XX - Emprego de Sensores de Fontes Humanas de IM; e
- EB70-MT-10.4XX - Emprego de Rec e Vig de Inteligência Militar.

Há, ainda, a previsão de atualização da Base Doutrinária do 6º Batalhão de Inteligência Militar - difusão no ano de 2024 - e a realização, também em 2024, dos seminários e reuniões para discussão da Contraineligência nas Operações; da Inteligência de Fontes Humanas; e da Geointeligência.

Por fim, também no PDDMT/2024, encontram-se estabelecidas as seguintes Necessidades de Conhecimentos Específicos (NCE) para a Doutrina:

- EB70-MC-10.356 - Inteligência Cibernética - Grupo de pesquisa: Guerra do Futuro, Inovação e Indústria de Defesa - prazo: até 2028.
- EB70-MC-10.213 - Operações de Informação - prazo: até 2028.

No contexto do Prg EE LUCERNA, é necessário destacar as seguintes ações (Brasil, 2020):

- Implementar capacidades de obtenção, integração e análise de dados em consonância com as novas demandas doutrinárias da F Ter, com vistas a atender um amplo espectro de operações, em situação de normalidade e crise - operações de guerra e não-guerra;
- Ampliar a difusão da Doutrina de Inteligência Militar nos Estabelecimentos de Ensino de Formação, Aperfeiçoamento e Altos Estudos; e
- Incrementar o ensino da Disciplina de Inteligência Militar nas escolas militares, especialmente no que diz respeito às fontes tecnológicas.

3.3.2 Organização

A razão de existir do SIEx é de pleno conhecimento de seus integrantes e dos consumidores de seus produtos. Além disso, há clareza e transparência das suas estruturas e processos. Isso significa que as responsabilidades de cada membro são bem definidas e comunicadas, garantindo que todos saibam o que se espera deles.

O SIEEx **produz, continuamente, os conhecimentos necessários para que o EB permaneça preparado e em condições de ser empregado contra quaisquer ameaças à soberania ou à integridade do país**, atuando em Operações no Amplo Espectro em atendimento às situações de emprego previstas na Constituição e na Estratégia Militar de Defesa.

A concepção do SIEEx é baseada em três funções gerais: obtenção, análise e suporte.

Os **meios de obtenção** atuam no Amb Op e no Espaço de Batalha, como sensores de dados sobre as ameaças e oportunidades existentes.

Os **meios de análise** produzem os conhecimentos que irão subsidiar os comandantes e seus estados-maiores, nos diversos níveis.

Os **meios de suporte** permitem a ligação dos meios de obtenção com os de análise, empregando a Tecnologia de Informação e Comunicações (TIC) (Brasil, 2015a, grifo próprio).

A presença de normas regulamentares torna o SIEEx um ente institucional sistematizado e funcional, com parâmetros que abrangem desde procedimentos operacionais até diretrizes éticas e legais orientadoras de suas atividades. Dentre outras, as seguintes normas encontram-se previstas na REPUBLICEx (Brasil, 2024):

- Normas de Ação para a Salvaguarda das Informações relacionadas com as Atividades de Inteligência do Sinal e de Guerra Eletrônica no âmbito do EB (NSISGE);
- EB60-IR-44.001 - Instruções Reguladoras para a Inscrição, a Seleção e a Matrícula (IRISM) nos Cursos de Especialização e no Estágio Geral da Escola de Inteligência Militar do Exército (EsIMEx); e
- R-65 - Regulamento da Escola de Inteligência Militar do Exército.

Especificamente no âmbito do Prg EE LUCERNA, ressaltam-se as seguintes diretivas (Brasil, 2020):

- Consolidar a implantação do 6º BIM;
- Implantar o núcleo do 1º;
- Implantar o núcleo do 4º BIM;
- Iniciar as atividades da EsIMEx em sua nova sede;
- Ampliação do número de vagas para os cursos e estágios/EsIMEx;
- Implementação do ensino de novas especializações na EsIMEx; e
- Prover a manutenção e melhoria das estruturas dos Grupos de Operações de Inteligência e das Companhias de Inteligência remanescentes e aumentar a capacidade dos meios de obtenção relacionados às fontes tecnológicas.

3.3.3 Adestramento

Atividade final da instrução militar na tropa, que objetiva a formação dos diversos agrupamentos de homens, com equipamentos e armamentos - pequenas

frações, frações, subunidades, unidades e grandes unidades - para a eventualidade de emprego, como instrumento de combate (Brasil, 2015b).

Ligados a este fator, tem-se, por exemplo, os seguintes programas-padrão - previstos no PDDMT/2024 (Brasil, 2023b) - que visam regulamentar o preparo dos integrantes e frações do SIEx para que possam ser empregados:

- EB70-PP-11.XXX - Programa-Padrão de Adestramento (PPA) do Batalhão de Inteligência Militar (BIM) - difusão em 2024;
- EB70-PP-11.XXX - Adestramento Básico da Companhia de Inteligência Militar (CIM) - difusão em 2025; e
- EB70-PP-11.XXX - Capacitação Técnica e Tática do Efetivo Profissional (CTTEP) do BIM e da CIM - difusão em 2026.

No que cabe ao Prg EE LUCERNA, tem-se o seguinte (Brasil, 2020):

- Incrementar o adestramento das estruturas de Inteligência Militar (IM) nos diversos escalões da Força Terrestre para atender à Função de Combate Inteligência em operações militares; e
- Desenvolver, nos diversos escalões da F Ter, módulos de adestramento dos meios de inteligência direcionados à exploração de dados de fontes tecnológicas.

3.3.4 **Material**

São todos os materiais e sistemas empregados no desempenho de suas atividades, havendo a necessidade de acompanhamento da evolução de tecnologias de emprego militar e com base na prospecção tecnológica em outros países ou mesmo nos ambientes acadêmicos ou em outros de natureza civil (Brasil, 2022a).

O desempenho da atividade de Inteligência certamente necessita de diversos materiais desde os mais simples até os mais modernos meios de obtenção e análise.

O manual EB20-MF-10.107 - Inteligência Militar Terrestre (Brasil, 2015a) trata dos meios necessários ao desenvolvimento das atividades e das tarefas ligadas à Inteligência Militar. Tais meios englobam não apenas o pessoal, como também os diversos materiais e recursos. Afinal, a definição de meios traz que são a força e os elementos materiais que integram o poder de combate (Brasil, 2015b).

Quanto a este fator, o Prg EE LUCERNA destaca as seguintes ações:

- Entregar às Estruturas de Inteligência dos diversos escalões modernos materiais de TIC, de monitoramento de dados das fontes de sinais, de cibernética e

de imagens e outros Sistemas e Materiais de Emprego Militar (SMEM) que atendam à transformação do SIEx;

- Mobiliar a EsIMEEx com materiais de TIC, de monitoramento de dados das fontes de sinais, de cibernética e de imagens e outros SMEM, que atendam à necessidade de especialização dos recursos humanos que mobiliarão o SIEx em sua fase de transformação;
- Exigir o compromisso de confidencialidade por parte dos fornecedores de equipamentos e *softwares* de tecnologia da informação e comunicações, Inteligência de Sinais, Imagens e Cibernética; e
- Priorizar a obtenção de material nacional, de modo a reduzir, ao máximo possível, a dependência externa.

3.3.5 Educação

Compreende todas as atividades continuadas de capacitação e habilitação, formais e não formais, destinadas ao desenvolvimento do indivíduo quanto à sua competência individual requerida (Brasil, 2022a).

Neste contexto, o SIEx, conforme estabelecido no Plano de Cursos e Estágios Gerais no EB (PCE-EB) para o ano de 2024 (Brasil, 2022b) e no PCE-EB para o ano de 2025 (Brasil, 2023c), oferece os seguintes cursos e estágios⁷, com a finalidade de preparar, requalificar e atualizar os seus quadros, os profissionais que ocuparão os cargos previstos e desempenharão as diversas funções no próprio SIEx:

- Curso Avançado de Inteligência;
- Curso Básico de Inteligência;
- Curso de Geointeligência - militares das Forças Armadas;
- Curso de Geointeligência - Forças Auxiliares, Nações Amigas e SISBIN;
- Curso de Inteligência Cibernética;
- Curso de Inteligência de Sinais; e
- Estágio Setorial de Inteligência Militar para o Sistema de Prontidão.

Neste aspecto, o Prg EE LUCERNA estabeleceu as seguintes ações:

- Prosseguir na implantação de novos cursos e estágios que atendam às necessidades resultantes da transformação do SIEx;

⁷ Todas as atividades de ensino e capacitação são reguladas separadamente pelas correspondentes Instruções Reguladoras para a Inscrição, a Seleção e a Matrícula (IRISM).

- Prosseguir na implementação e validação dos processos de capacitação dos usuários dos meios TIC, de monitoramento de dados das fontes de sinais, cibernética e imagens, observadas as tecnologias que atendam à transformação do SIEx;
- Orientar, em coordenação com o Departamento-Geral do Pessoal (DGP), de acordo com a legislação vigente, a seleção de pessoal para os cursos e estágios da EsIMEx, pressupondo o imediato preenchimento de cargos no SIEx; e
- Propor e participar da atualização dos currículos dos Cursos de Formação, Aperfeiçoamento e Altos Estudos, de forma a incrementar o estudo da Disciplina IM, em coordenação com o Departamento de Educação e Cultura do Exército (DECEX).

3.3.6 **Pessoal**

O fator pessoal abrange todas as atividades relacionadas aos integrantes da Força, nas vertentes: planejamento de carreira, movimentação, preenchimento de cargos, higidez física, avaliação e valorização do mérito profissional e moral. É uma abordagem que engloba o planejamento, coordenação, organização, direção, controle e validação das competências ligadas à dimensão humana (Brasil, 2022a).

O SIEx é composto pelos órgãos e pelas **pessoas** do próprio EB que, sob a responsabilidade dos comandantes, estão envolvidos na execução das atividades e tarefas de inteligência ou ligados à sua regulamentação (Brasil, 2015a, grifo próprio).

Quanto a este fator e como prova da constante busca da evolução diante dos novos desafios, o PDDMT/2024 prevê a elaboração do novo Quadro Organizacional do Batalhão de Inteligência Militar (BIM), para difusão em 2025 (Brasil, 2023b).

Observado o Prg EE LUCERNA, tem-se as seguintes orientações:

- Implementar a racionalização dos cargos nos Quadros de Cargos (QC) e nos Quadros de Cargos Previstos (QCP) das estruturas do SIEx, com a finalidade de atender o processo de transformação do SIEx; e
- Implementar a racionalização dos cargos nos QC e QCP da EsIMEx para atender o incremento de especializações a serem conduzidas em sua nova sede.

3.3.7 **Infraestrutura**

Engloba todos os elementos estruturais - instalações físicas, equipamentos e serviços necessários - que dão suporte ao preparo e ao emprego dos elementos, de acordo com a especificidade de cada um e os requisitos funcionais (Brasil, 2022a).

O SIEx se **estrutura** em todos os escalões do Exército Brasileiro a fim de produzir os conhecimentos necessários a cada um dos níveis decisórios. Os **meios de obtenção** podem ser especializados ou não especializados. Os especializados, existentes nas OM de Inteligência de cada escalão - no âmbito do SIEx, são também designados como Órgãos de Inteligência (OI) - empregam técnicas operacionais específicas para a busca de dados. Os não especializados, orgânicos das OM subordinadas de cada comando, realizam ações de reconhecimento e vigilância. Os **meios de análise** materializam-se na Seç Intlg - 2ª Seção - de cada OM apoiada em sua Central de Inteligência Militar (CIM). A 2ª Seção de OM também é designada como Agência de Inteligência (AI) no âmbito do SIEx. (Brasil, 2015a, grifo próprio).

Como exemplo da aplicação deste fator na incorporação de capacidades pelo SIEx, destacam-se as seguintes iniciativas previstas na REPUBLEx (Brasil, 2024):

- EB20-D-03.050 - diretriz para a implantação do núcleo do 1º Batalhão de Inteligência Militar por transformação da 1ª Companhia de Inteligência;
- Port Nr 1.030 - C Ex, de 9 OUT 20 - transformação da 1ª Companhia de Inteligência em 1º Batalhão de Inteligência Militar e ativação do seu núcleo;
- EB20-D-03.062 - diretriz para a implantação do núcleo do 4º Batalhão de Inteligência Militar por transformação da 4ª Companhia de Inteligência;
- Port Nr 1.580 - C Ex, de 31 AGO 21 - criação do núcleo do 4º Batalhão de Inteligência Militar por transformação da 4ª Companhia de Inteligência; e
- EB20-D-03.072 - diretriz para a implantação do Grupo de Operações de Inteligência (GOI) no 1º Grupamento de Engenharia.

Por fim, em relação a este fator, o Prg EE LUCERNA estabeleceu (Brasil, 2020):

- Concluir as obras da nova EsIMEx; e
- Entregar a infraestrutura física necessária às Estruturas de Inteligência dos diversos escalões da Força Terrestre por meio de obras de Engenharia - ampliação, readequação ou construção.

3.4 CONSIDERAÇÕES FINAIS SOBRE O SIEx - MATRIZ SWOT

O SIEx apresenta pontos fortes e oportunidades, entretanto também enfrenta desafios e ameaças que devem gerenciados ou superados. Todos esses aspectos são apresentados e categorizados no APÊNDICE a este trabalho segundo os critérios utilizados pela Técnica de Análise Estruturada (TAE) conhecida como Matriz SWOT⁸.

⁸ SWOT corresponde ao acrônimo para *Strengths, Weaknesses, Opportunities and Threats* - Forças, Fraquezas, Oportunidades e Ameaças. É uma técnica de análise estruturada analítica, enquadrada na categoria Apoio à Decisão, que, em português, é conhecida como Matriz FFOA (Brasil, 2019).

4 PROPOSTA PARA O IMPLEMENTO DA MASINT NO SIEx

O Exército Brasileiro gera forças por meio da incorporação das capacidades necessárias para combater ameaças concretas e potenciais ao Estado, as quais são elencadas por meio da análise da conjuntura e com base em cenários prospectivos.

Por sua vez, a capacidade é obtida a partir da interação sinérgica dos fatores determinantes do DOAMEPI, que são Doutrina, Organização, Adestramento, Material, Educação, Pessoal e Infraestrutura (Brasil, 2022a).

A análise do SIEx revela uma estrutura robusta, com uma forte base doutrinária e esforços de modernização e capacitação. Porém, também revela um sistema que enfrenta desafios, como a dependência tecnológica e a necessidade de coordenação eficiente entre suas várias partes. Ainda, é um ente com grandes oportunidades para avançar, especialmente através da integração de novas tecnologias e parcerias, e que precisa estar preparado para enfrentar ameaças cibernéticas e cenários com duras restrições financeiras que podem impactar suas operações e desenvolvimento.

Assim, da análise da matriz *SWOT*, tem-se as seguintes estratégias e ações que podem ser consideradas para o implemento da MASINT no SIEx:

4.1 DOCTRINA

4.1.1 Atualização e integração da doutrina existente

- Incorporar a MASINT à base doutrinária do SIEx, absorvendo, de maneira integrada, os seus novos princípios, técnicas e procedimentos;
- Por meio da inclusão de novos itens e orientações, adequar as diretrizes do Prg EE LUCERNA às necessidades específicas da MASINT, permitindo que essa disciplina também seja atendida; e
- Incorporar procedimentos de avaliação e monitoramento contínuo da eficácia da doutrina de MASINT, promovendo ajustes e mudanças para garantir sua relevância e adaptabilidade às mudanças no ambiente operacional e tecnológico.

4.1.2 Desenvolvimento de normas e procedimentos

- Produzir e implementar normas específicas para as operações no campo da MASINT, definindo as responsabilidades e os métodos de coleta, de análise e de disseminação de informações;

- Estabelecer critérios para identificação e avaliação de fontes de dados da MASINT, fornecendo orientações claras sobre como selecionar e priorizar recursos para a coleta que melhor atendam às necessidades operacionais apresentadas; e
- Estabelecer protocolos de segurança e proteção de informações sensíveis da MASINT, garantindo o manuseio adequado e a salvaguarda dos dados coletados, de acordo com os padrões de segurança do SIEx e com a legislação pertinente.

4.1.3 Normas referentes à capacitação e ao treinamento

- Desenvolver planos e programas-padrão de formação e de adestramento em MASINT, aproveitando a infraestrutura de educação contínua já existente;
- Garantir que as lições aprendidas e melhores práticas observadas durante a elaboração e o aperfeiçoamento do processo de ensino em MASINT sejam usadas na retroalimentação - e aprimoramento - do sistema; e
- Permitir que a EsIMEx tenha a necessária flexibilidade quanto a alterações do programa de ensino da MASINT até que haja a consolidação deste, segundo o que é esperado do profissional concludente da capacitação.

4.1.4 Documentação e manuais operacionais

- Elaborar produtos doutrinários dedicados à MASINT como foi feito, por exemplo, em favor da Inteligência de Sinais e da Geointeligência. Neles deverão ser tratados temas desde a definição de conceitos até a estruturação de protocolos de análise e disseminação de informações; e
- Assegurar que esses documentos possam ser regularmente atualizados de forma que os avanços tecnológicos possam ser rapidamente incorporados.

4.1.5 Interoperabilidade Doutrinária

- Incluir diretrizes para a cooperação e o compartilhamento de informações entre as diversas agências de inteligência integrantes do SISBIN, fomentando o desenvolvimento de uma abordagem integrada e colaborativa no uso da MASINT que facilite o enfrentamento de ameaças e desafios comuns; e
- Assegurar, até o ponto em que não haja prejuízos ao SIEx, que a doutrina MASINT seja compatível com a de outras agências de inteligência integrantes do SISBIN, facilitando a cooperação e troca de informações.

4.2 ORGANIZAÇÃO

4.2.1 Estruturação de equipes, frações ou módulos especializados

- Nos diversos escalões do SIEx e de acordo com o nível de conhecimento exigido para a operação dos equipamentos e sistemas, readequar a alocação dos cargos previstos com as correspondentes habilitações exigíveis ou desejadas; e
- Estruturação, no órgão central do SIEx, de uma célula dedicada à gestão e coordenação das atividades na área de MASINT, com atribuições claras e recursos adequados para garantir o funcionamento efetivo e integrado desse novo tipo de inteligência com as disciplinas já existentes e exploradas no SIEx.

4.2.2 Integração com outras Disciplinas de Inteligência

- Inicialmente no órgão central do SIEx e, mais tarde, nos demais escalões da F Ter, estabelecer uma estrutura que permita o trabalho de equipes multidisciplinares para a condução de análise dos dados obtidos por MASINT, envolvendo profissionais de diferentes áreas e de outras Disciplinas de Inteligência para uma compreensão abrangente das informações coletadas, expansão do conhecimento sobre MASINT na Comunidade de Inteligência e o seu consequente ganho de importância; e
- Aproveitar a interconexão existente com outras agências para fortalecer a colaboração em projetos na área da MASINT.

4.2.3 Expansão geográfica

- De forma gradual e aproveitando a ampla cobertura geográfica do SIEx, expandir a estrutura de MASINT, procurando observar as lições aprendidas e as melhores práticas em cada etapa dessa expansão, visando utilizar de maneira efetiva e mais segura os recursos a serem empregados na fase subsequente; e
- Assegurar que as equipes especializadas em MASINT em cada região tenham a capacidade de operar de forma autônoma e, ao mesmo tempo, coordenada e integrada junto à célula congênere existente no CIE, órgão central do SIEx.

4.2.4 Cargos e carreiras

- Como se trata de uma disciplina que necessita de pessoal altamente especializado, elaborar e propor planos de carreira específicos ou atrativos para os

profissionais de MASINT, incentivando a especialização e promovendo a retenção de talentos na área; e

- Designar pessoal qualificado e especializado para coordenar e executar as operações no campo da MASINT, incluindo analistas de inteligência, técnicos em sensoriamento remoto e engenheiros de sistemas, dentre outros.

4.2.5 Estrutura de apoio

- Estruturar equipes de apoio técnico e administrativo dedicadas ao suporte das operações no campo da MASINT, garantindo recursos adequados para suas atividades; e
- Estabelecer parcerias, convênios e acordos de cooperação com entidades civis, públicas ou privadas para a manutenção dos sistemas e dos equipamentos utilizados em MASINT.

4.3 ADESTRAMENTO

4.3.1 Programas de Adestramento Avançado (PAA)

- Elaborar programas de capacitação específicos para garantir a retenção dos conhecimentos adquiridos na capacitação, para que os profissionais de MASINT estejam continuamente preparados para lidar com as particularidades da coleta, processamento e análise de dados de MASINT;
- Estabelecer o monitoramento e a avaliação contínuos dos programas de capacitação em MASINT, permitindo identificar áreas de sucesso e oportunidades de melhoria. Ao analisar o impacto e a eficácia desses programas, o SIEx pode ajustar suas estratégias de treinamento para garantir que atendam às necessidades da organização e de seus profissionais; e
- Promover a participação das equipes, frações ou módulos especializados nos adestramentos avançados, principalmente na fase da Simulação Construtiva, ou em outras atividades diversas dos Comandos Militares de Área.

4.3.2 Treinamento prático e simulações

- Implementar exercícios práticos e simulações que permitam ao pessoal de MASINT praticar as técnicas em ambientes controlados;

- Realizar exercícios práticos e simulações envolvendo dados de MASINT - mesmo que não estejam disponíveis os meios de obtenção dessa disciplina de Inteligência - proporcionando aos participantes a experiência e o ambiente para o desenvolvimento das habilidades para, de forma efetiva, lidar com as situações que envolvam os conhecimentos obtidos por meio de MASINT;
- Participação em grandes exercícios internacionais em que haja a aplicação das técnicas e dos conhecimentos de MASINT; e
- Realizar treinamento junto à Marinha do Brasil e à Força Aérea Brasileira aproveitando os seus recursos, uma vez que, em determinado grau, essas forças singulares já utilizam diversos meios MASINT.

4.3.3 **Certificação e qualificação**

- Estabelecer um sistema de certificação para operadores dos sistemas MASINT, assegurando que todos os profissionais atendam aos padrões necessários, devendo haver a reciclagem sempre que for necessário; e
- Estimular e promover a qualificação contínua, com revisões periódicas das habilidades e dos conhecimentos dos profissionais envolvidos com MASINT.

4.3.4 **Parcerias educacionais como oportunidades de adestramento**

- Estabelecer parcerias com instituições acadêmicas e de pesquisa para que o pessoal envolvido com MASINT auxilie no desenvolvimento ou aprimoramento de produtos e, ao mesmo tempo, mantenha o seu adestramento nos procedimentos e técnicas de MASINT; e
- Estimular a participação de especialistas - nacionais ou estrangeiros - nas atividades de adestramento em MASINT, de forma a enriquecer os programas de treinamento e agregar novas perspectivas.

4.3.5 **Adestramento em segurança cibernética**

- Incluir módulos de treinamento em segurança cibernética nos programas de treinamento e adestramento em MASINT, preparando o pessoal para a proteção de dados sensíveis e o enfrentamento de ameaças digitais; e
- Realizar adestramento em conjunto com a Inteligência Cibernética, visando preparar os operadores de MASINT também para as ameaças do ambiente virtual.

4.4 MATERIAL

4.4.1 Investimento em tecnologia avançada

- Investir em tecnologia de ponta para sistemas e equipamentos de MASINT, como sensores, sistemas de monitoramento e plataformas de análise de dados e produção de conhecimento; e
- Modernizar e constantemente atualizar os diversos sistemas para garantir a efetividade e a confiabilidade das ações em MASINT, incluindo aí a atualização de *softwares* e de sistemas de armazenamento de dados e a manutenção regular de equipamentos de forma a assegurar o seu funcionamento adequado.

4.4.2 Atualização de infraestrutura

- Modernizar a infraestrutura física e tecnológica do SIEx para suportar as operações de MASINT, garantindo um ambiente operacional seguro e eficiente; e
- A manutenção de estoques de peças de reposição e de equipamentos de *backup* garante a disponibilidade contínua de recursos essenciais para as operações de MASINT. Isso reduz o risco de interrupções nas atividades de inteligência devido a falhas técnicas ou indisponibilidade de equipamentos e assegura a continuidade das operações em qualquer cenário.

4.4.3 Parcerias Público-Privadas

- Desenvolver parcerias com os setores público e privado para obter acesso a tecnologias inovadoras e recursos adicionais para emprego em MASINT. Acordos com empresas especializadas permitem que a organização acompanhe os avanços tecnológicos e rapidamente os implemente no SIEx;
- Estabelecer acordos com os fornecedores de tecnologia para garantir a reposição de equipamentos críticos sempre for necessário;
- Em parceria com o meio acadêmico, desenvolver ferramentas específicas para a análise e a interpretação de dados de MASINT, permitindo que o SIEx extraia *insights* valiosos para a sustentação do conhecimento a ser utilizado na tomada de decisões; e
- Criar laboratórios de pesquisa e desenvolvimento dedicados à MASINT em parceria com outras instituições, oferecendo um ambiente controlado para que se

possa testar e validar novas tecnologias e metodologias de análise de dados. Esses laboratórios serviriam como centros de excelência onde os especialistas do SIEx poderiam colaborar com pesquisadores acadêmicos e da indústria para impulsionar a inovação e o desenvolvimento de capacidades em MASINT, que, ainda, poderiam ser utilizadas em outras áreas.

4.4.4 **Segurança da informação**

- Implementar medidas rigorosas de segurança para proteger os dados e sistemas de MASINT contra ameaças internas e externas, desenvolvendo, ainda, procedimentos de proteção e controle de acesso para assegurar a integridade das informações;

- Implementar sistemas de gestão de informação integrados, permitindo o armazenamento, organização e compartilhamento de dados de MASINT no âmbito do SIEx e com outras agências de inteligência. Isso promove a colaboração e a troca de informações entre diferentes unidades e aumenta a eficiência das operações de inteligência em todo SISBIN;

- Realizar testes e avaliações de segurança cibernética para identificar e mitigar vulnerabilidades nos sistemas e infraestrutura de TI do SIEx. Ao simular cenários de ataque e avaliar a resposta da organização, é possível fortalecer as defesas cibernéticas e garantir a proteção dos dados e informações sensíveis de MASINT; e

- Implementar políticas e procedimentos de gerenciamento de ativos de TI garante a manutenção e o uso eficiente dos recursos tecnológicos em MASINT. Isso inclui a definição de diretrizes para a aquisição, a manutenção e o desfazimento de equipamentos.

4.4.5 **Integração de sistemas**

- Garantir a compatibilidade e a integração dos novos sistemas de MASINT com as tecnologias já existentes, facilitando a troca de informações e a coordenação operacional no âmbito do SIEx; e

- Realizar avaliações e testes para assegurar que os novos equipamentos atendam aos requisitos operacionais e de segurança e que não comprometam os sistemas já estabelecidos.

4.5 EDUCAÇÃO

4.5.1 Currículos voltados para MASINT

- Aproveitando a estrutura da EsIMEx, conduzir cursos e estágios - ou incluir módulos de ensino nas atividades de capacitação já existentes - com currículos e programas especificamente voltados para a MASINT, incluindo tanto disciplinas que abordem aspectos teóricos quanto matérias dedicadas às práticas em MASINT; e
- A elaboração dos programas e currículos para obtenção das habilidades em MASINT deve garantir que os profissionais estejam preparados para lidar com as particularidades dessa disciplina, compreendendo os princípios e aplicações dessa área, ficando em condições de melhor enfrentar as ameaças e desafios operacionais relacionados à análise de dados de MASINT.

4.5.2 Programas de pós-graduação e especialização

- Buscar e oferecer programas de pós-graduação e cursos de especialização em MASINT em parceria com universidades e centros de pesquisa; e
- Incentivar o desenvolvimento acadêmico do pessoal integrante do SIEx em MASINT.

4.5.3 *Workshops* e seminários

- Organizar *workshops* e seminários sobre MASINT, pelo menos até que se tenha essa disciplina de Inteligência consolidada no SIEx, trazendo especialistas nacionais e internacionais para compartilhar conhecimentos e práticas; e
- Participar de intercâmbios com instituições especializadas, permitindo aos integrantes do SIEx oportunidades valiosas de aprendizado e aprofundamento em MASINT. Estágios, colaborações em projetos de pesquisa e acesso a recursos acadêmicos podem enriquecer a formação dos profissionais e fortalecer a expertise do SIEx nessa área específica de inteligência.

4.5.4 Educação continuada

- Desenvolver, mesmo que em plataformas de ensino a distância, programas de educação continuada que permitam aos profissionais de MASINT atualizar seus conhecimentos e habilidades regularmente; e

- No ambiente da Biblioteca Digital do Exército, oferecer acesso a artigos e outros produtos sobre MASINT para os profissionais do SIEx.

4.5.5 Pesquisas e publicações

- Fomentar a pesquisa aplicada em MASINT, incentivando a publicação de artigos e estudos sobre MASINT em revistas científicas e conferências e financiando projetos que possam trazer inovações e melhorias educacionais e operacionais; e
 - Nos cursos da EsIMEEx em que há a produção de conhecimento, como no Curso Avançado de Inteligência, distribuir os aspectos ligados à implementação da MASINT no SIEx - base teórica, material a ser adquirido e proposta para o conteúdo de cursos ou estágios, dentre outros - permitindo o seu estudo aprofundado.

4.6 PESSOAL

4.6.1 Seleção

- Selecionar profissionais com formação e experiência relevantes em áreas correlatas à MASINT, como física, engenharia, geografia e ciência da computação, visando garantir a disponibilidade de talentos qualificados para atuar nesse campo especializado de inteligência;
 - Estabelecer critérios de seleção que levem em conta habilidades técnicas e a capacidade de lidar com tecnologias avançadas; e
 - Como se trata de uma área que exige elevada capacitação, estabelecer programas de capacitação e de desenvolvimento de carreira para os profissionais interessados em se especializar em MASINT por meio da oferta de oportunidades de formação acadêmica, treinamento prático e certificações reconhecidas.

4.6.2 Retenção de talentos

- Oferecer incentivos e benefícios para reter talentos na área de MASINT, incluindo bônus, oportunidades de desenvolvimento profissional;
 - Promover a valorização e reconhecimento dos profissionais de MASINT, destacando suas contribuições para o SIEx; e
 - Estímulo à participação dos profissionais do SIEx em redes de colaboração e comunidades de prática relacionadas à MASINT, tanto em âmbito nacional quanto

internacional, visando fortalecer sua expertise e permitindo a atualização sobre as tendências e os avanços na área.

4.6.3 Capacitação contínua

- Investir na capacitação contínua do pessoal envolvido nas atividades de MASINT, oferecendo cursos de atualização e especialização;
- Utilizar treinamentos práticos e simulações para manter as habilidades operacionais em alto nível; e
- Estabelecer convênios e parcerias com instituições de ensino e pesquisa, com órgãos governamentais e com empresas privadas que possam contribuir para o desenvolvimento e o aperfeiçoamento das capacidades MASINT do SIEx, através do compartilhamento de conhecimento, recursos e melhores práticas.

4.7 INFRAESTRUTURA

4.7.1 Desenvolvimento de instalações especializadas

- Observada a necessidade de se planejar detalhadamente a expansão do emprego de MASINT, construir e equipar instalações especializadas para operações nesse campo sem negligenciar a segurança - seja na obtenção, na transmissão ou em outra atividade - e com foco na efetividade operacional. Deve-se assegurar que tais instalações estejam estrategicamente localizadas ao longo da extensa cobertura geográfica abrangida pelo SIEx, complementando suas capacidades de vigilância e monitoramento de áreas de interesse; e
- Investir na aquisição ou atualização de equipamentos e de tecnologias para coleta, processamento e análise de dados de MASINT, garantindo a disponibilidade de recursos adequados e suficientes para suportar as atividades de manutenção preventiva ou corretiva dos diversos sistemas.

4.7.2 Manutenção e atualização de infraestruturas

- Atualizar as infraestruturas existentes para garantir que estejam seguras e operacionais mesmo com a inserção de uma nova Disciplina de Inteligência;
- Implementar programas de manutenção preventiva a fim de se evitar falhas e maximizar a vida útil de equipamentos e sistemas;

- Sem comprometimento do sistema já existente e em funcionamento, prover sistemas de armazenamento e gestão de dados escaláveis e flexíveis, que permitam o gerenciamento eficiente e seguro de grandes volumes de informações advindas de diversas fontes de MASINT; e
- Estabelecer protocolos e procedimentos que padronizem e regulamentem a gestão e manutenção da infraestrutura de MASINT do SIEx, incluindo cronogramas de manutenção, atualização de *software* e *hardware* e gestão de incidentes, visando garantir a disponibilidade e confiabilidade dos sistemas em operação.

4.7.3 **Segurança física e tecnológica**

- Fortalecer as medidas de segurança física e tecnológica nas instalações de MASINT para a proteção contra ameaças externas e internas; e
- Adaptar a infraestrutura de comunicação e conectividade, permitindo o ágil e seguro intercâmbio de informações e dados obtidos por meio de MASINT entre as diferentes unidades e escalões do SIEx.

4.7.4 **Investimento em tecnologias emergentes**

- Investir em tecnologias emergentes que possam melhorar a eficiência e a capacidade das operações no campo da MASINT ou, ainda, monitorar os avanços tecnológicos que representem a possibilidade para integrar novas soluções; e
- Desenvolver ferramentas e plataformas especializadas em visualização e análise de dados de MASINT, que possam facilitar a interpretação e o entendimento das informações coletadas, subsidiando a produção de conhecimento e a tomada de decisões.

4.7.5 **Parcerias para o desenvolvimento de tecnologias e infraestruturas**

- Buscar parcerias com instituições privadas e com o setor acadêmico para conjuntamente desenvolver tecnologias e infraestruturas ligadas à MASINT; e
- Promover parcerias públicas para o compartilhamento de infraestrutura e de recursos tecnológicos, visando otimizar investimentos, reduzir custos e ampliar as capacidades operacionais do SIEx em relação à MASINT.

5 CONCLUSÃO

A implementação da Inteligência por Assinatura de Alvos, também conhecida como MASINT - *Measurement and Signature Intelligence* - no Sistema de Inteligência do Exército (SIEEx) é um importante marco para a modernização e o fortalecimento das capacidades ligadas à Inteligência Militar.

Ao longo das seções anteriores, foram explorados os fundamentos teóricos da MASINT, suas aplicações potenciais e as oportunidades e desafios associados à sua efetiva integração ao SIEEx.

O Exército Brasileiro, reconhecendo a importância crescente das Disciplinas de Inteligência tidas como “tecnológicas” - sinais, imagens, cibernética e assinatura de alvos, por exemplo - enfrenta o desafio de integrar a MASINT em sua estrutura de inteligência sem, contudo, comprometer a sinergia e efetividade já observada no sistema.

Nesse contexto, a partir da análise da estrutura do SIEEx, momento em que foram levantadas suas características internas - que o fortalecem ou enfraquecem - e as oportunidades e ameaças do ambiente externo que o circundam, passou-se à elaboração de estratégias e ações baseadas nos fatores do DOAMEPI para permitir a inserção da MASINT em sua estrutura.

No âmbito da doutrina, propôs-se a atualização e integração dos conceitos e procedimentos e técnicas relativos à MASINT, além do estabelecimento de normas e protocolos específicos para as atividades nessa área. Neste ponto, destaca-se a necessidade de uma abordagem multidisciplinar e colaborativa na qual sejam observadas as peculiaridades tanto do ambiente interno do SIEEx quanto das outras agências de inteligência e instituições externas também partícipes do SISBIN.

Observou-se também que a organização do SIEEx deve ser reajustada para acomodar os sistemas e as equipes especializadas em MASINT, possibilitando a integração com as demais disciplinas de inteligência. Além disso, constatou-se que a expansão geográfica gradual e planejada dos meios e recursos MASINT ao longo da estrutura da Força Terrestre é fundamental para a adequada e efetiva incorporação dessa nova capacidade.

No que tange ao adestramento, concluiu-se que é essencial a elaboração de programas específicos para a capacitação continuada dos profissionais de MASINT, incluindo treinamentos práticos e simulações. Ainda, que a recorrente certificação e

qualificação dos operadores e a inclusão de módulos de segurança cibernética nos programas de treinamento são medidas complementares importantes no esforço de manter a prontidão operacional e a confiabilidade dos conhecimentos produzidos.

Quanto ao material, identificou-se que o investimento em tecnologia avançada e infraestrutura adequada é crucial para o sucesso das atividades e operações no âmbito da Inteligência por Assinatura de Alvos, uma vez que capacitará o SIEx a coletar, processar, analisar e disseminar informações e conhecimentos de maneira eficiente e segura.

No que tange ao fator educação, verificou-se que este desempenha um papel fundamental na consolidação da MASINT no SIEx. Planos de ensino e currículos especialmente dedicados e programas de pós-graduação que procuram despertar o interesse pela pesquisa aplicada nessa área fomentam a discussão sobre o tema e são recursos essenciais para a capacitação e atualização dos profissionais.

Ainda, salientou-se que convênios e parcerias público-privadas que permitam o desenvolvimento conjunto e colaborativo de laboratórios ou centros de pesquisa são estratégias-chave para garantir o acesso a tecnologias inovadoras e promover o desenvolvimento de capacidades, mesmo em meio a um cenário caracterizado por restrições orçamentárias.

Na vertente do pessoal, viu-se que a valorização da carreira e o estímulo no intuito de que seja possível reter talentos na atividade de MASINT são necessários em uma área na qual se exige elevado conhecimento e capacitação técnica de nível.

Quanto ao aspecto infraestrutura, percebeu-se que - quando for necessário e observando a gradual implantação de módulos MASINT no SIEx - é crucial que esse permita a instalação e operação de robustos sistemas de TI nos quais possam, de maneira segura, ser armazenados, processados e transmitidos grandes volumes de dados.

Em síntese, a implementação bem-sucedida da MASINT no SIEx exigirá um esforço conjunto e coordenado, envolvendo atualização doutrinária, reestruturação organizacional, investimento em capacitação e tecnologia e colaboração estratégica com instituições externas ao Sistema de Inteligência do Exército.

Também no que tange à análise do SIEx, salienta-se que as ações propostas segundo os diversos fatores do DOAMEPI visam não apenas promover a efetiva implementação da MASINT, mas também mitigar os riscos e desafios associados a essa integração.

Ainda, ao estudar os pontos fortes e oportunidades que foram identificados, fica evidente que a MASINT, tal qual ocorreu durante sua consolidação na estrutura de Estado norte-americana, pode contribuir de maneira substancial para a obtenção de inteligência estratégica e tática sobre diferentes áreas de interesse, seja de aplicação militar ou não.

Por fim, verificou-se que o incremento de sistemas de gestão da informação integrados a eficazes protocolos de segurança cibernética garantirá que os dados obtidos por MASINT sejam protegidos contra ameaças, enquanto políticas claras de compartilhamento e disseminação de informações promoverão a interoperabilidade e a cooperação com outras agências e parceiros de inteligência.

Conclui-se, assim, que há uma série de estratégias e ações a serem adotadas antes que o Exército Brasileiro, em especial o SIEEx, possa, de fato, utilizar todas as capacidades atreladas a essa Disciplina de Inteligência no fortalecimento de sua capacidade operacional, ficando em condições de enfrentar os desafios do ambiente contemporâneo.

REFERÊNCIAS

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei Nr 9.883, de 7 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência (ABIN), e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm. Acesso em: 5 abr. 2024.

BRASIL. Decreto nº 5.484, de 30 de junho de 2005. Aprova a Política de Defesa Nacional, e dá outras providências. **Diário Oficial da União**, Brasília, DF, p. 5, 1º jul. 2005. Disponível em <https://legislacao.presidencia.gov.br/atos/?tipo=DEC&numero=5484&ano=2005&ato=5baUzZU5UMRpWTd9b>. Acesso em 5 abr. 2024.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército (EME). **Inteligência Militar Terrestre** - EB20-MF-10.107. 2ª ed. Brasília, DF, 2015a.

BRASIL. Ministério da Defesa (MD). Estado-Maior Conjunto das Forças Armadas (EMCFA). **Glossário das Forças Armadas** - MD35-G-01. 5ª ed. Brasília, DF, 2015b.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei Nr 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm. Acesso em: 5 abr. 2024.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército (EME). **Portaria Nr 272, de 12 de julho de 2017**. Aprova a Diretriz de Iniciação do Programa Estratégico do Exército (Prg EE) LUCERNA e constitui a equipe que confeccionará o Estudo de Viabilidade do Programa.

BRASIL. Ministério da Defesa (MD). Exército Brasileiro. Comando de Operações Terrestres (COTER). **Produção do Conhecimento de Inteligência** - EB70-MT-10.401. 1ª ed. Brasília, DF, 2019.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército (EME). **Portaria Nr 140, de 7 de julho de 2020**. Aprova a Diretriz de Implantação do Programa Estratégico do Exército (Prg EE) LUCERNA (EB20-D-08.040).

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército (EME). **Doutrina Militar Terrestre** - EB20-MF-10.102. 3ª ed. Brasília, DF, 2022a.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército (EME). **Plano de Cursos e Estágios Gerais no EB (PCE-EB) para o ano de 2024** - PCE-EB/2024. Brasília, DF, 2022b.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei Nr 11.693, de 6 de setembro de 2023**. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência. Brasília, DF, 2023a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm. Acesso em: 5 abr. 2024.

BRASIL. Ministério da Defesa (MD). Exército Brasileiro. Comando de Operações Terrestres (COTER). **Plano de Desenvolvimento da Doutrina Militar Terrestre (PDDMT)/2024** - EB70-P-10.001. Brasília, DF, 2023b.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército (EME). **Plano de Cursos e Estágios Gerais no EB (PCE-EB) para o ano de 2025** - PCE-EB/2025. Brasília, DF, 2023c.

BRASIL. Ministério da Defesa (MD). Exército Brasileiro. Secretária-geral do Exército. **Relação de Publicações do Exército (REPUBLEx)**. Brasília, DF, 2024.

CANHAM, Matthew. **Neurosecurity**: human brain electro-optical signals as MASINT. *American Intelligence Journal*, vol. 36, no. 2, 2019, pp. 40-47. Disponível em: <https://www.jstor.org/stable/27066371>. Acesso em 5 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA (EUA). Câmara dos Representantes. Comitê Permanente de Inteligência. **IC21: The Intelligence Community in the 21st Century**. Washington, DC, 1996. Disponível em: <https://www.govinfo.gov/app/details/GPO-IC21/context>. Acesso em: 5 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. Office of the Director of National Intelligence (ODNI). **MASINT: A surface level look into a misunderstood intelligence discipline**. Washington, D.C., 2022. Disponível em: https://www.dni.gov/files/ODNI/documents/21-113_MASINT_Primer__2022.pdf. Acesso em 5 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA (EUA). Headquarters. Department of the Army. **Intelligence** - FM 2-0. Washington, D.C., 2023.

LOWENTHAL, Mark M.; CLARK, Robert Morris. **The five disciplines of intelligence collection**. 1st ed. Thousand Oaks, California, EUA: Sage Publications, 2015.

MORRIS, John L. MASINT: An "INT" Still in Transition. **American Intelligence Journal**, v. 36, n. 2, p. 21-27, 2019. Disponível em: <https://www.jstor.org/stable/27066369>. Acesso em 5 abr. 2024.

RICHELSON, Jeffrey T. MASINT: The New Kid in Town. **International Journal of Intelligence and CounterIntelligence**, p. 149-192, 2001. Disponível em: <https://doi.org/10.1080/088506001300063136>. Acesso em 5 abr. 2024.

SENG, Aaron Chia Eng. **MASINT: The Intelligence of the Future**. Defence Science and Technology Agency (DSTA), Singapore, 2007. Disponível em: <https://docplayer.net/54952044-Masint-theintelligence-of-the-future.html>. Acesso em: 5 abr. 2024.

SINGH, Neil. A Guide to Measurement and Signature Intelligence (MASINT). **Grey Dynamics**. S.l., 2023. Disponível em https://greydynamics.com/a-guide-to-measurement-and-signature-intelligence-masint/#30_How_is_MASINT_collected. Acesso em 5 abr. 2024.

APÊNDICE A - Análise do SIEx empregando a Matriz SWOT

1 PONTOS FORTES

- Base doutrinária consolidada - o SIEx possui uma base doutrinária sólida, como evidencia o conjunto de documentos normativos, de orientação e de ensino, que abrangem desde princípios gerais até detalhes operacionais específicos;
- Capacidade de produzir conhecimento - capacidade robusta de produção de conhecimento, evidenciada pelos diversos produtos doutrinários e normativos;
- Organização estruturada - existe uma clara estrutura organizacional, com funções bem definidas e responsabilidades atribuídas, garantindo transparência e eficiência ao sistema;
- Adestramento e educação contínuos - o sistema investe em programas de adestramento e educação para manter seu pessoal atualizado e capacitado para enfrentar os desafios que estão sempre em surgimento;
- Infraestrutura avançada - há um esforço para modernizar a infraestrutura, incluindo a criação de novas unidades e a atualização de instalações, garantindo que o SIEx tenha os recursos físicos necessários para operar de maneira efetiva;
- Capacidade de adaptação - o SIEx demonstra possuir uma capacidade de adaptação às demandas em constante mudança, como evidenciado pelo Programa Estratégico LUCERNA, que visa transformar e modernizar o sistema para enfrentar os complexos e atuais desafios, bem como os que estão por vir;
- Tradição e experiência - o Exército Brasileiro possui uma longa tradição e experiência na atividade de Inteligência;
- Ampla cobertura geográfica - a presença do SIEx em todos os escalões do EB garante uma cobertura geográfica abrangente, algo vantajoso para a coleta e análises focadas nos aspectos ambientais das diversas regiões do país;
- Interconexão com outras agências - há integração com outras agências de inteligência por meio do Sistema Brasileiro de Inteligência (SISBIN), permitindo o intercâmbio de informações e experiências; e
- Tecnologia - investir em tecnologia da informação e de comunicações, bem como em sistemas de monitoramento e cibernética, permite ao SIEx aumentar sua capacidade de coleta e análise de dados e estar junto à vanguarda no que tange às operações de inteligência.

2 OPORTUNIDADES

- Novas áreas de especialização - a incorporação de novas especializações, conforme estabelecido pelo Prg EE LUCERNA, a exemplo da inteligência cibernética e da geointeligência, mostra como o SIEEx utiliza uma oportunidade para expandir suas capacidades e abordar novos desafios;
- Inovação tecnológica - o avanço da tecnologia oferece oportunidades para desenvolver as capacidades de obtenção, análise e suporte do SIEEx, especialmente com relação às fontes tecnológicas;
- Cooperação interinstitucional - o SIEEx pode aproveitar parcerias com outras agências de inteligência e instituições acadêmicas buscando compartilhar recursos, conhecimentos e melhores práticas;
- Desenvolvimento profissional - investir no desenvolvimento profissional e contínuo do pessoal do SIEEx (por meio da própria EsIMEEx ou de outras instituições) pode melhorar sua eficácia e resiliência diante dos desafios emergentes;
- Desenvolvimento de Parcerias Público-Privadas (PPP) - explorar parcerias com o setor privado ou mesmo com outras instituições públicas pode criar oportunidades para acesso a tecnologias inovadoras e a recursos adicionais que complementarão as capacidades já existentes no SIEEx;
- Modernização de infraestrutura - investimentos contínuos na modernização da infraestrutura física e tecnológica podem melhorar significativamente a eficiência e a segurança das operações de inteligência;
- Incremento de capacidades - a implementação dos projetos do Prg EE LUCERNA pode fortalecer e expandir as capacidades do SIEEx, garantindo a eficácia operacional frente a novas ameaças;
- Melhoria de processos - revisar e otimizar os processos internos, tornando-os mais efetivos. A simplificação e a automação de procedimentos podem reduzir a burocracia, agilizar a tomada de decisões e otimizar as operações do SIEEx;
- Internacionalização - estabelecer parcerias internacionais permite a troca de conhecimento e de melhores práticas, permitindo incorporar novas estratégias e tecnologias ao SIEEx e enriquecendo suas capacidades;
- Desenvolvimento em segurança cibernética - o ambiente cibernético é um componente cada vez mais relevante nas operações de inteligência. A expansão das capacidades nessa área é crucial para proteger infraestruturas críticas.

3 PONTOS FRACOS

- Dependência de recurso externo - a dependência de fornecedores externos pode representar um desafio, especialmente no tocante a termos de segurança e de confiabilidade de equipamentos e sistemas;
- Necessidade constante de atualização - o rápido avanço da tecnologia e das ameaças exige uma constante atualização e evolução da doutrina, organização, treinamento e equipamentos do SIEx para permanecer relevante e eficaz. Técnicas consagradas, mas obsoletas e não efetivas devem ser abandonadas, mesmo que haja forte resistência interna a mudanças;
- Dependência de recursos financeiros - a disponibilidade de recursos dita os avanços que podem ser feitos no campo da inteligência. Restrições orçamentárias limitam o SIEx quanto ao investimento em inovação e modernização, impactando, dessa forma, a capacidade do sistema de enfrentar ameaças;
- Integração complexa - a integração de novos sistemas e tecnologias com as estruturas já existentes pode ser um desafio significativo. A complexidade técnica e a necessidade de compatibilidade entre diferentes plataformas podem atrasar a implementação e reduzir a eficácia operacional;
- Dependência de normas e regulamentos - embora a existência de normas e regulamentos seja importante para garantir legalidade e legitimidade às operações do SIEx, uma dependência excessiva desses documentos pode levar à rigidez e à dificuldade de adaptação a novas situações ou tecnologias emergentes;
- Segurança da informação - a proteção da confidencialidade e integridade das informações é um desafio contínuo, especialmente com a introdução de novas tecnologias. Procedimentos de cunho humano ou técnico devem ser constantemente aprimorados para proteger contra ameaças internas e externas;
- Burocracia e lentidão processual - a estrutura burocrática e hierarquizada e os processos lentos podem dificultar a resposta rápida e tempestiva contra ameaças emergentes, bem como a adoção de novas tecnologias e estratégias;
- Capacidade limitada de capacitar - por diversos motivos e razões, há saída de pessoal do SIEx, além disso, o sistema tem sido expandido. No entanto, a oferta para capacitações é limitada ou de elevado custo, podendo resultar na escassez de pessoal qualificado para atender às demandas crescentes de inteligência, quer seja quanto à quantidade de profissionais, quer seja quanto ao conhecimento exigido;





- Racionalização de cargos - a racionalização dos cargos para acompanhar a transformação do SIEx pode encontrar obstáculos. A reestruturação de funções pode gerar resistência e dificuldades na adaptação dos quadros existentes; e
- Dependência de Fontes Humanas - a obtenção informações empregando operações típicas da Inteligência de Fontes Humanas possui elevado risco e pode representar uma vulnerabilidade que deve ser considerada no planejamento e na decisão pela execução ou não de uma ação dessa natureza.

4 AMEAÇAS

- Cibersegurança - o aumento de ameaças no espaço cibernético representa um desafio significativo para a segurança das operações de inteligência do SIEx;
- Espionagem e contrainteligência - a crescente sofisticação das atividades de espionagem e contrainteligência requer vigilância contínua para proteger as operações do SIEx contra interferências externas;
- Instabilidade política - a estruturação de um efetivo sistema de inteligência leva tempo. Assim, eventos imprevisíveis ou decisões inesperadas consequentes da instabilidade política podem representar a descontinuidade de projetos e programas e afetar a capacidade do sistema em oferecer respostas confiáveis e tempestivas;
- Instabilidade social - a instabilidade social - surgida inclusive de um possível cenário de instabilidade política - pode criar um ambiente volátil que coloca pressão adicional sobre as operações de inteligência do SIEx;
- Guerra de informação - a sensibilidade do material tratado no âmbito do SIEx faz com que seus produtos sejam alvo de constantes ameaças que procuram acessar tais temas para a exploração segundo seus interesses;
- Vazamento de informações sensíveis - a possibilidade de vazamento de informações sensíveis representa uma ameaça à integridade e confiabilidade de todo o SIEx, exigindo medidas rigorosas de segurança e de controle de acesso;
- Acelerada evolução tecnológica - a rápida evolução tecnológica representa um desafio para o SIEx, que precisa acompanhar as mudanças e integrar novas tecnologias de maneira eficaz, evitando uma defasagem operacional;
- Dependência de fornecedores - a dependência de fornecedores externos para tecnologias críticas pode ser uma vulnerabilidade. Problemas de fornecimento ou questões de segurança podem impactar negativamente o SIEx;

- **Regulamentação** - a rigidez regulamentar pode impactar as operações e a flexibilidade do SIEEx. Por outro lado, a adaptação a novas regras pode ser um processo complexo e longo, afetando a capacidade operacional; e
- **Competição global** - a competição internacional na área de inteligência é intensa. Há o desenvolvimento de tecnologias, metodologias e culturas em diversos países. Manter-se na vanguarda dessa competição exige investimento contínuo em inovação e capacitação, além da sinergia de diversos setores públicos e privados.

Tabela 1 - O Sistema de Inteligência do Exército - Matriz SWOT

<p style="text-align: center;">PONTOS FORTES (+)</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> • Base doutrinária consolidada; • Cpcd de produzir conhecimento; • Organização estruturada; • Adestramento e educação contínuos; • Infraestrutura avançada; • Capacidade de adaptação; • Tradição e experiência; • Ampla cobertura geográfica; • Interconexão com outras agências; e • Tecnologia de ponta. 	<p style="text-align: center;">FRAQUEZAS (-)</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> • Dependência de recurso externo; • Nec constante de atualização; • Dependência de recursos financeiros; • Integração complexa; • Dependência legal; • Segurança da informação; • Burocracia e lentidão processual; • Capacidade limitada de capacitar; • Racionalização de cargos; e • Dependência de Fontes Humanas.
<p style="text-align: center;">OPORTUNIDADES (+)</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> • Novas áreas de especialização; • Inovação tecnológica; • Cooperação interinstitucional; • Desenvolvimento profissional; • Desenvolvimento de PPP; • Modernização de infraestrutura; • Incremento de capacidades; • Melhoria de processos; • Internacionalização; e • Desenvolvimento em Seg cibernética. 	<p style="text-align: center;">AMEAÇAS (-)</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> • Cibersegurança; • Espionagem e contrainteligência; • Instabilidade política; • Instabilidade social; • Guerra de informação; • Vazamento de informações sensíveis; • Acelerada evolução tecnológica; • Dependência de fornecedores; • Rígida regulamentação; e • Competição global.

Fonte: Compilação do autor⁹.

⁹ Compilação feita a partir das diversas obras utilizadas como fonte de consulta para a elaboração deste trabalho.