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

CURSO AVANÇADO DE INTELIGÊNCIA PARA OFICIAIS

TRABALHO DE CONCLUSÃO DE CURSO

A ESTRUTURAÇÃO DA OSINT, COMO DISCIPLINA DE INTELIGÊNCIA, NO ÂMBITO DO SIEx

Brasília
2024

Ten Cel CELSO AUGUSTO CARVALHO **SAMPAIO**

A ESTRUTURAÇÃO DA OSINT, COMO DISCIPLINA DE INTELIGÊNCIA, NO ÂMBITO DO SIEx

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

Orientador: Maj **RODRIGO** ANDRADE CERQUEIRA

Brasília
2024

S192e Sampaio, Celso Augusto Carvalho

A estruturação da OSINT, como disciplina de inteligência, no âmbito do SIEx. / Celso Augusto Carvalho Sampaio – 2024.
47 f.

Orientador: Rodrigo Andrade Cerqueira
Trabalho de Conclusão de Curso (Especialização em Análise de Inteligência) - Escola de Inteligência Militar do Exército (EsIMEx), Brasília – DF, 2024.

1. Inteligência de fontes abertas 2. OSINT 3. Estruturação
4. DOPEMAI I. Título.

Ten Cel CELSO AUGUSTO CARVALHO **SAMPAIO**

A ESTRUTURAÇÃO DA OSINT, COMO DISCIPLINA DE INTELIGÊNCIA, NO ÂMBITO DO SIEx

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

Aprovado em 18 de junho de 2024.

COMISSÃO DE AVALIAÇÃO:

_____
RENATO SERGIO BARBOSA **PASSERI** - Ten Cel – Presidente
Escola de Inteligência Militar do Exército

_____
DIOGO **DUTTON** TAVARES - Ten Cel – Membro
Escola de Inteligência Militar do Exército

_____
RODRIGO ANDRADE CERQUEIRA - Maj – Membro
Escola de Inteligência Militar do Exército

AGRADECIMENTOS

A Deus, por me permitir prosseguir na vida com saúde e felicidade.

À minha família, pelo constante incentivo, amor incondicional e compreensão em todos os momentos, sendo fundamental para a conclusão deste trabalho.

Ao Maj Rodrigo, pela orientação segura e oportuna, paciência e atenção durante a confecção deste trabalho.

Aos meus companheiros de curso, pela camaradagem e pelo excelente relacionamento profissional.

“Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece, mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas...” (Sun Tzu)

RESUMO

Na Era da Informação, a Inteligência de Fontes Abertas (Open-Source Intelligence – OSINT, em inglês) vem ganhando importância no âmbito da comunidade de inteligência mundial. O volume exponencial de dados encontrados em informações publicamente disponíveis ou gerados pelos usuários da Web nas redes sociais ou em plataformas digitais vem fomentando o desenvolvimento dos serviços de obtenção, análise e difusão de conhecimentos de inteligência, no contexto de uma Metodologia de Produção do Conhecimento. Além disso, a coleta de dados e informações em fontes abertas tem sido a base inicial dos trabalhos das disciplinas de inteligência que buscam dados protegidos. Dessa forma, os avanços necessários à adequada estruturação dos fatores determinantes da capacidade da Disciplina de Inteligência OSINT (doutrina, organização, pessoal, educação, material, adestramento e infraestrutura – DOPEMAI), no âmbito do Sistema de Inteligência do Exército Brasileiro (SIEx), estão relacionados, particularmente, à implementação de equipes de analistas especializados em OSINT, ampliando a capacidade das instituições para coletar e analisar informações oriundas de grandes quantidades de dados. Nesse sentido, o presente trabalho tem como objetivo contribuir com o processo de atualização da doutrina de Inteligência Militar do Exército Brasileiro, no contexto da integração da OSINT com as demais disciplinas de inteligência, aprimorando a produção e difusão de conhecimentos oportunos ao processo decisório do cliente.

Palavras-chave: Inteligência de fontes abertas. OSINT. Estruturação. DOPEMAI.

ABSTRACT

In the Information Age, Open-Source Intelligence (OSINT) has been gaining importance within the global intelligence community. The exponential volume of data accessible in publicly available information or generated by web users on social networks or digital platforms has been encouraging the development of services for collection, analyzing and disseminating intelligence knowledge, in the context of an Analysis Process. Furthermore, the collection of data and information from open sources has been the initial basis for the work of intelligence disciplines that seek protected data. In this way, the advances necessary for the adequate structuring of the factors determining the capacity of the OSINT as Intelligence Discipline (doctrine, organization, personnel, education, material, training and infrastructure – DOPEMAI), within the scope of the Brazilian Army Intelligence System (SIEx), are particularly related to the implementation of teams of analysts specialized in OSINT, expanding the capacity of institutions to collect and analyze information from large amounts of data. In this sense, the present work aims to contribute to the process of updating the Brazilian Army's Military Intelligence doctrine, in the context of integrating OSINT with other intelligence disciplines, improving the production and dissemination of timely intelligence for the client's decision-making process.

Keywords: Open-source Intelligence. OSINT. Structuring. DOPEMAI.

SUMÁRIO

CELSO AUGUSTO CARVALHO SAMPAIO[1]

1 INTRODUÇÃO

A Doutrina de Inteligência Militar Terrestre brasileira define a Inteligência de Fontes Abertas (Open-Source Intelligence – OSINT) como a Inteligência baseada em informações coletadas de fontes de caráter público. Dadas as suas peculiaridades de coleta de informações em fontes publicamente disponíveis, a sua importância se revela em reduzir ou complementar as demandas das demais disciplinas de Inteligência, sendo, portanto, considerada a fonte básica de Inteligência (Brasil, 2015, p. 3-3).

Com o surgimento da internet, em 1993, a OSINT expandiu sua relevância e oportunidade no âmbito da atividade de Inteligência. A OSINT é a fonte de Inteligência dominante para a maioria dos analistas. Clark destaca que, nos Estados Unidos, a quantidade de inteligência derivada de OSINT foi estimada em cerca de 80% (Clark, 2022, p. 367, tradução nossa).

Nesse escopo, é valido salientar que as disciplinas de Inteligência proporcionam capacidades variadas, eficazes e complexas, que requerem formação e experiência para compreendê-las plenamente, em todos os escalões. Cada disciplina de Inteligência possui especificidades em termos de autoridades, doutrina, requisitos de formação, pontos fortes e vulnerabilidades de coleta, técnicas de emprego, estrutura de força, terminologia, canais técnicos, meios de gestão de missão e capacidades de apoio ao processo de exploração e disseminação (Estados Unidos, 2023, p. 1-16, tradução nossa).

Clark (2014, tradução nossa) afirma que a chave para compreender a coleta de informações é vê-la como um sistema complexo e aplicar metodologia de sistemas ao examiná-la, caracterizando sua função, processo e estrutura. A função determina o que um sistema produz e para quem. Na coleta, isso significa determinar quem são os clientes, o que é produzido para eles, os propósitos que o produto serve e quão valioso ele é para eles. O processo refere-se a como as informações passam pela fase de coleta até chegar aos clientes. A estrutura refere-se a como um sistema é organizado e por quê.

[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. sampa297@gmail.com

Atualmente, o Sistema de Inteligência do Exército Brasileiro (SIEx) carece de uma adequada estruturação dos fatores determinantes da capacidade da Disciplina de Inteligência OSINT (doutrina, organização, pessoal, educação, material, adestramento e infraestrutura – DOPEMAI), aspecto este que delimita o problema visualizado no presente trabalho.

Segundo Geiger (2022, p.12, tradução nossa) a relevância da OSINT, nos dias atuais, emana muito além da simples informação. A OSINT requer um conjunto de competências especializadas para uma coleta segura e adequada de informações, implicando em técnicas, táticas e procedimentos (TTP), processos, tecnologias, ferramentas e formas de disseminação personalizadas. Desta forma, destaca-se a importância do presente estudo, uma vez que seus resultados contribuirão para a atualização da estrutura organizacional da OSINT, no âmbito do SIEx.

Nesse escopo, este trabalho tem por objetivo estudar um modelo de estruturação da Inteligência de Fontes Abertas, no âmbito do SIEx, como forma de impulsionar a OSINT ao mesmo patamar de relevância das demais disciplinas de Inteligência. Para tanto, a investigação tem como objetivos específicos o levantamento das peculiaridades relacionadas à efetividade da OSINT na comunidade de Inteligência, bem como a atual situação do seu emprego no SIEx, chegando a uma proposta de organização estrutural para a disciplina.

A realização do presente estudo foi precedida de uma revisão da literatura que norteia a Inteligência de Fontes Abertas (OSINT), com destaque para o seu emprego na Inteligência Militar. Em seguida, o presente trabalho baseou-se em uma pesquisa qualitativa, quanto à forma de abordagem, e exploratória, quanto ao objetivo geral. Os resultados do trabalho foram apoiados, ainda, pelo instrumento de coleta de dados do tipo questionário, direcionado ao universo de especialistas em Inteligência Militar.

Como forma de ambientar o leitor, o trabalho foi dividido nas seguintes seções: introdução; a OSINT; a situação atual da OSINT no SIEx; discussão e, por fim, a conclusão.

2 A OSINT

Open-source Intelligence – OSINT é a Inteligência produzida a partir de informações publicamente disponíveis e coletada, explorada e divulgada em tempo hábil para um público apropriado, com o objetivo de atender a um requisito específico de Inteligência. A OSINT é empregada por coletores treinados e certificados, que usam ferramentas, processos e análises para gerar Inteligência operacionalmente relevante a partir da vasta quantidade e variedade de informações publicamente disponíveis (Estados Unidos, 2023, p. 1-19, tradução nossa).

A Inteligência de fontes abertas abrange as fontes tradicionais publicadas e transmitidas que estão normalmente disponíveis para qualquer pessoa: meios de comunicação como jornais, revistas, rádio, televisão; material profissional e acadêmico de conferências, simpósios, associações profissionais e trabalhos acadêmicos; relatórios governamentais e dados oficiais. Atualmente, também inclui o conteúdo da Web gerado pelo usuário, como sites de redes sociais, sites de compartilhamento de vídeos, wikis e blogs (Clark; Mitchell, 2019, tradução nossa).

Alinhado a esse conceito, Gack (2022, p. 19, tradução nossa) destaca que “as redes sociais agora compreendem informações publicamente disponíveis em quase dois bilhões de websites ativos, cinco bilhões de perfis de redes sociais e bilhões de usuários diários, oferecendo um tesouro de dados de fonte aberta”.

Na doutrina conjunta do Reino Unido, a OSINT possui um conceito estendido, dadas as peculiaridades do avanço informacional da atualidade, sendo definida como:

> Inteligência derivada de informações publicamente disponíveis, bem como outras informações não classificadas que têm distribuição ou acesso público limitado. Isto abrange os processos de coleta e análise de informação publicamente disponível para apoiar funções de Inteligência, bem como a produção de produtos de OSINT dedicados. Informação publicamente disponível é descrita como qualquer informação onde haja uma base razoável para acreditar que foi legalmente disponibilizada ao público em geral. Isto inclui: todas as informações disponíveis online, incluindo aquelas frequentemente referidas como informações de fonte aberta; qualquer material publicado ou transmitido para consumo do público em geral; informações disponíveis mediante solicitação a um membro do público em geral; informações legalmente vistas ou ouvidas por qualquer observador casual ou disponibilizadas em uma reunião aberta ao público em geral; e informações cujo acesso é limitado, como aquelas disponibilizadas mediante um acesso pago, de fóruns exclusivos para membros ou por serem consideradas “informações de propriedade coletadas por uma empresa comercial” (Reino Unido, 2023, p. 81, tradução nossa).

Neste quesito, cabe destacar que Gack (2022, p. 18, tradução nossa) incluiu no conceito de OSINT:

> informações oriundas de volumes em massa e dados de conteúdo em plataformas públicas; indicadores de localização, incluindo pistas textuais e recursos de fundo; informações de redes sociais, com base no conteúdo do usuário e na interação online; exploração de metadados incorporados em arquivos digitais, incluindo imagens e vídeos; exploração de dados de transações, incluindo transferências de blockchain de moeda estrangeira; detecção de bots, utilizando volume de transmissão e padrões de transmissão online; e exploração de conteúdos da dark web, incluindo a utilização de ferramentas comerciais de indexação (Gack, 2022, p. 18, tradução nossa).

Além do processo de encontrar, selecionar e adquirir informações de fontes publicamente disponíveis, Clark (2014, p. 53, tradução nossa) ressaltou que a sistemática de tradução e a análise de material em língua estrangeira, também é uma ação de OSINT.

2.1 A IMPORTÂNCIA DA OSINT

A globalização e a necessidade crescente de governos, ONGs e empresas comerciais adquirirem informações em todo o mundo alimentaram uma indústria que fomentou a evolução da OSINT, dos anos 1990 aos dias atuais. Atualmente, muitas empresas fornecem informações de fonte aberta em todo o mundo, formando o que tem sido chamado de “comunidade de inteligência do setor privado”. Quatro dessas empresas são as empresas norte-americanas Stratfor e Intellibridge e as empresas britânicas Jane’s Information Group e Oxford Analytica (Clark, 2014, p. 82, tradução nossa).

Nessa conjuntura, Clark (2022, p. 386, tradução nossa) ressalta que, nas ações de coleta ou de busca de todas as fontes de Inteligência, o erro mais comum tem sido o de desvalorizar a importância da OSINT, uma vez que é a fonte de maior disponibilidade e facilidade de coleta, sendo, por isso, considerada a menos valiosa. Corroborando a assertiva acima, Gack (2022, p. 20, tradução nossa) defende a ideia de que a OSINT, “representa a maior, mais barata e mais acessível fonte de Inteligência do mundo, revelando-se inestimável para as operações de Segurança Nacional dos Estados Unidos”.

Ainda nessa linha de raciocínio, Clark (2014, p. 54, tradução nossa) estabelece que a fonte aberta tem duas funções na Inteligência: servir como fonte de um produto de Inteligência acabado; e acionar ou validar a coleta por outra fonte de Inteligência, como a Inteligência de Comunicações (COMINT) ou a Inteligência de Fontes Humanas (HUMINT). Na concepção do autor, os analistas de todas as fontes devem

começar pela OSINT, porque é muito barato e fácil de usar, e não devem recorrer a recursos de coleta mais caros até esgotarem o potencial do OSINT.

No contexto da vasta quantidade de informações em fontes abertas, Geiger (2022, p. 10, tradução nossa) exemplifica que, em março de 2020, eram gerados, diariamente, aproximadamente 2,5 exabytes[2] de dados na internet, representando volumes de dados valiosos em tempo real. O autor reforça que um profissional experiente e com habilidades específicas pode navegar por esse terreno superlotado para rastrear informações personalizadas para um conjunto de problemas específicos, preencher lacunas de Inteligência e direcionar os esforços de coleta e de busca de outras disciplinas de Inteligência.

Geiger (2022, p. 11, tradução nossa) ressalta que a evolução do domínio do ciberespaço e das capacidades de Inteligência Artificial (IA) colocarão a OSINT na vanguarda das capacidades de um comandante, na obtenção de consciência situacional, além de fortalecer as relações e a partilha de informações com parceiros e aliados estrangeiros, ao mesmo tempo que fornece atualizações de informações quase em tempo real aos combatentes.

Coerente com as assertivas acima, que convergem para a importância da OSINT, na atualidade, serão explorados aspectos relacionados às peculiaridades que conferem um caráter de complexidade relacionada ao emprego da Inteligência de Fontes Abertas.

2.2 PECULIARIDADES DA OSINT

2.2.1 OSINT: fonte e disciplina de Inteligência

A OSINT se comporta ora como Fonte de Inteligência, ora como Disciplina de Inteligência. Para melhor entender os conceitos de fonte e disciplina de Inteligência, a Joint Doctrine Publication 2-00 (Reino Unido, 2023, p. 51, tradução nossa) estabelece que fonte é uma linha de comunicação, como um agente humano ou um canal de comunicação interceptado, e que a disciplina representa um método ou técnica de coleta (HUMINT ou SIGINT, por exemplo). Pode-se ter múltiplas fontes em uma única disciplina.

[2] Exabyte (EB) é um múltiplo de byte, que é a unidade de tamanho de arquivo para armazenar informações digitais. Um exabyte equivale a cerca de um milhão de terabytes (TB) (disponível em https://pt.wikipedia.org/wiki/Exabyte).

De acordo com o Field Manual 2-0 (Estados Unidos, 2023, p. 1-15, tradução nossa), uma disciplina de Inteligência é uma área bem definida de planejamento, coleta, exploração, análise e relatórios de Inteligência, usando uma categoria específica de recursos técnicos ou humanos.

2.2.2 Vulnerabilidades da OSINT

Na Era da Informação[3], muitas são as vulnerabilidades a que os analistas de OSINT estão expostos ao coletarem e analisarem informações oriundas de fontes abertas. Na Dimensão Informacional, onde o conteúdo está repleto de ações de negação, engano e dissimulação, Clark (2022, p. 470, tradução nossa) relata que a "OSINT desfruta de pouca ou nenhuma proteção, porque o material de origem não é classificado".

Clark (2014, tradução nossa) enfatiza que a fonte aberta é uma excelente forma de um serviço hostil realizar ações de engano ou enviar um sinal ao oponente, dada a certeza do seu recebimento pelo serviço adversário. Com isso, Clark cita que algumas das verificações padrão feitas na validação dos dados de OSINT são: precisão; credibilidade e autenticidade; oportunidade; e viés (Clark, 2014, tradução nossa).

Outra vulnerabilidade é apontada por Le Deuff (2021, tradução nossa), que destaca que o acesso aos dados de OSINT também depende da capacidade do investigador de OSINT para localizar informações, interpretá-las e, às vezes, inferi-las. Para Le Deuff (2021, p. 2, tradução nossa), "a OSINT constitui um novo regime de verdade que se baseia no estudo de vestígios para estabelecer evidências que sustentem uma lógica demonstrativa e explicativa, em particular, para responder à desinformação".

No contexto dos riscos a que a coleta de OSINT expõe os analistas norte-americanos, Potter e Bembenek (2022, p. 7, tradução nossa) evidenciam o risco de que, uma vez que os adversários dos EUA identifiquem os sites onde os analistas estão conduzindo pesquisas, eles comecem a adicionar informações falsas a esses sites ou a criar um redirecionamento para sites falsos. Outro risco potencial apontado pelos autores é que os proprietários de sites e governos estrangeiros podem identificar

[3] A era da informação (também conhecida como era computacional, era digital, era do silício ou era da nova mídia) é um período histórico de rápida mudança das indústrias tradicionais para uma economia centrada na Tecnologia da Informação (disponível em https://pt.wikipedia.org/wiki/Era_da_informacao).

que um militar ou unidade específica dos EUA acessou suas informações, causando incidentes diplomáticos.

No intuito de mitigar as vulnerabilidades do emprego da OSINT, o Exército dos Estados Unidos da América (US Army) está constantemente buscando e revendo novas ferramentas e tecnologias para auxiliar na coleta e priorização, concentrando-se na construção de um exército totalmente integrado com a comunidade de OSINT para expandir o compartilhamento de dados, agilizar a tomada de decisões e aprimorar o uso de recursos de nuvem para incluir IA em evolução, análise semântica e serviços e ferramentas de aprendizado de máquina (Geiger, 2022, tradução nossa).

2.2.3 O especialista de OSINT

Os profissionais OSINT devem ser capazes de realizar a triagem e validar grandes quantidades de dados. Eles devem eliminar desinformação, propaganda, influência maligna estrangeira, vieses e relatórios circulares em níveis inimagináveis, sem qualquer interação pessoal, enquanto tentam determinar a qualidade da informação (Geiger, 2022, tradução nossa). Geiger (2022, tradução nossa) ressalta, ainda, que “os profissionais OSINT devem possuir habilidades para navegar através da Deep Web e da Dark Web, para coletar as informações mais aplicáveis às suas Necessidades de Inteligência”.

Os profissionais de OSINT devem utilizar tecnologia, como IA e aprendizagem automática, para criar e utilizar algoritmos que possam deslocar montanhas de dados para responder a requisitos específicos de Inteligência. Os profissionais da OSINT também devem manter uma vasta familiaridade tanto com o domínio do ciberespaço como com o ambiente de informação, ter uma compreensão da governação de dados e do funcionamento interno da Internet integral, e ser dotados de capacidades concebidas para filtrar rapidamente exabytes de dados (Geiger, 2022, tradução nossa).

Na seara da necessidade de especialização do profissional de OSINT, o *US Army Intelligence Center of Excellence – USAICoE* desenvolveu seis módulos de treinamento para todos os analistas de Inteligência sobre metodologias de pesquisa de fontes abertas e fundamentos da internet com foco nos rastros que os analistas deixam quando conduzem pesquisas on-line (Potter; Bembeneck, 2022, p.6, tradução nossa).

O Exército Australiano desenvolveu um treinamento contínuo de OSINT por meio da participação em uma série de cursos de OSINT com aliados militares e treinamento de fornecedores comerciais, permitindo a formação de analistas generalistas de OSINT (Hopper, 2022, tradução nossa).

Considerando a conjuntura de emprego da OSINT nas Forças de Defesa do Canadá, os especialistas em OSINT são tão cruciais para o conceito de integração de todas as fontes quanto os de HUMINT, de SIGINT ou de IMINT. Dessa forma, difunde-se a ideia de que a realização de pesquisas na internet sem o uso de ferramentas especializadas e técnicas avançadas pode revelar informações sobre a instituição, razão pela qual existem políticas para proibir o uso negligente da internet para a coleta de informações (Holtz; Maxwell, 2022, tradução nossa).

2.2.4 A célula de OSINT

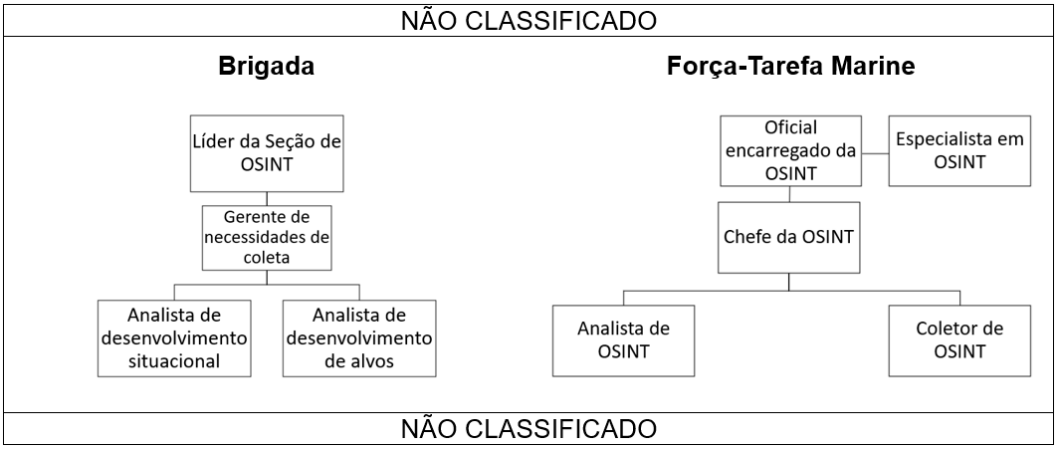
Diante da possibilidade da composição de células de OSINT nas estruturas organizacionais das Forças Armadas, consta do Manual Técnico ATP 2-22.9 do Departamento de Defesa (DoA) dos EUA:

> "O Comandante ou a Seção de Inteligência **poderá organizar recursos OSINT**, conforme necessário, para atender aos requisitos da missão. A equipe de inteligência deve equilibrar as necessidades adicionais de OSINT com as necessidades de outras disciplinas de inteligência e capacidades de inteligência complementares. Qualquer formação de uma **célula OSINT** desvia o pessoal de outras tarefas e requisitos de inteligência.
> As opções disponíveis para organizar um recurso OSINT incluem a formação de uma **célula dedicada de analistas OSINT** e treinar analistas selecionados em todas as disciplinas de inteligência para aproveitar a OSINT e satisfazer as necessidades de inteligência (Estados Unidos, 2017, p. 2-1, tradução nossa, grifo nosso)."

Segundo a doutrina acima, a estruturação da célula de OSINT varia de acordo com o escalão. O Manual Técnico ATP 2-22.9 aponta exemplos de composição de células de OSINT no nível Brigada e inferiores[4], conforme a Figura 1 (Estados Unidos, 2017, tradução nossa).

[4] Brigade Combat Team (BCT) e Marine Air-Ground Task Force (MAGTF), frações básicas de emprego do Exército dos EUA (US Army) e dos Marines (US Marines Corps) – (Estados Unidos, 2017, tradução nossa).

Figura 1 – Exemplo de organização da Célula de OSINT no nível Brigada e inferiores



Fonte: Estados Unidos (2017, p.2-2 e 2-3, tradução nossa).

2.2.5 Integração da OSINT com outras fontes e disciplinas

Acerca da capacidade de integração da OSINT com as demais fontes de Inteligência, visando ao refinamento do produto a ser difundido ao cliente, a Joint Doctrine Publication 2-00 ratifica o conceito da Inteligência multidisciplinar como a fusão de informações extraídas de mais de uma fonte ou de duas ou mais disciplinas de coleta. De acordo com a doutrina inglesa, a integração de duas ou mais disciplinas de Inteligência distintas, visa à melhoria da qualidade do produto de Inteligência (Reino Unido, 2023, tradução nossa).

No mesmo sentido, a doutrina norte-americana define que a coleta das diversas disciplinas de Inteligência é integrada durante o gerenciamento da coleta para garantir uma abordagem multidisciplinar, que apoia a análise eficaz da Inteligência e, em última análise, a Inteligência de todas as fontes. Por sua vez, a Inteligência de todas as fontes facilita a compreensão situacional precisa, a tomada de decisões e o apoio à segmentação (Estados Unidos, 2023, tradução nossa).

A integração da OSINT ocorre mais facilmente nas estruturas centralizadas de Inteligência, uma vez que comporta células de várias disciplinas de Inteligência. Nesse enquadramento, Clark frisa que uma organização centralizada é mais adequada para grandes Agências de Inteligência (CIA, por exemplo), onde a coleta deve lidar com uma diversidade de fontes. Considerando que esses grandes centros de Inteligência coletam informações de diferentes fontes, grande parte deste material só faz sentido

quando integrado para produzir um produto acabado[5] de Inteligência (Clark, 2014, tradução nossa).

Coerente com a doutrina do DoA/EUA, Geiger (2022, p.12, tradução nossa) defende que a OSINT nunca substituirá outras disciplinas de Inteligência, mas melhorará, ampliará e orientará seus esforços. Na concepção de Geiger (2022, p.12, tradução nossa), a OSINT é “o canto e a borda do quebra-cabeça que ajuda a indicar quais peças são necessárias para preencher o centro e completar o quadro – é a fonte de primeiro recurso”.

2.2.6 Processamento da OSINT

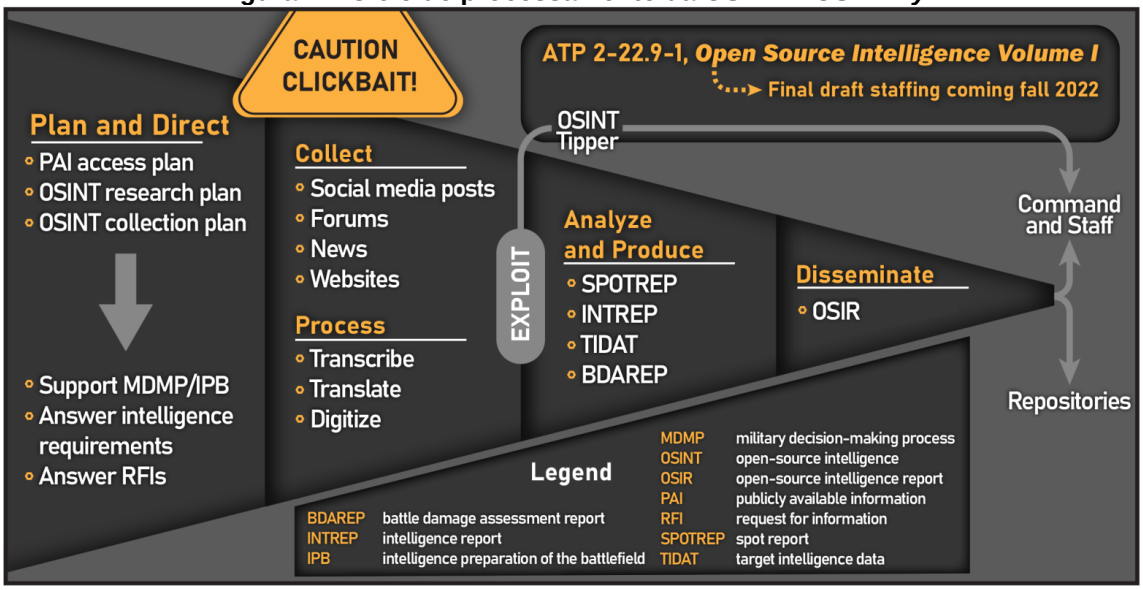
No intuito de descrever o faseamento do processo de produção da Inteligência de fontes abertas, Clark (2014, p. 63, tradução nossa) estabeleceu que, numa ordem linear, os principais passos são: planejamento e identificação das fontes; coleta e validação; processamento/tradução; análise; e disseminação. O autor destaca que embora tal processamento seja descrito como uma sequência linear, os analistas de OSINT possuem a flexibilidade de voltar às etapas anteriores ou avançar etapas adiante (Clark, 2014, tradução nossa).

No caso dos produtos diários de OSINT do Comando de Inteligência das Forças Canadenses, o processamento é precedido pela conversão e refino das informações coletadas, seguindo-se das etapas de processamento, exploração e disseminação (processing, exploitation and dissemination – PED), aproximando-se da doutrina defendida por Clark (2014) (Holtz; Maxwell, 2022, tradução nossa).

Na doutrina da OSINT no Exército dos Estados Unidos da América, o ciclo de processamento da OSINT se dá em quatro fases: planejamento e direção; coleta e processamento; análise e produção; e disseminação (Gack, 2022, p. 22, tradução nossa).

[5] Conhecimento produzido com a participação de todas as disciplinas de Inteligência na metodologia de produção do conhecimento, tornando-se, assim, mais completo possível sobre uma situação (Clark, 2022, tradução nossa).

Figura 2 – Ciclo de processamento da OSINT – *US Army*



Fonte: Gack (2022, p. 22).

2.2.7 O produto de OSINT deve ser difundido oportunamente

A doutrina do Exército dos Estados Unidos estabelece que os coletores/especialistas de OSINT produzem os seguintes produtos independentes de OSINT: o **Relatório de OSINT** (também conhecidos como OSIR – Open-source Intelligence Report), que podem ser incorporados em Estimativas de Inteligência, Resumos de Inteligência (INTSUMs), Estimativas de Execução de Inteligência e outros; e o **Relatório Tático de OSINT** (Estados Unidos, 2023, tradução nossa, grifo nosso).

De acordo com a doutrina acima, os produtos de OSINT também podem ser categorizados por uso e finalidade pretendidos. As categorias podem se sobrepor e as informações de OSINT podem ser usadas em mais de um produto. Dessa forma, os Relatórios de OSINT do Exército dos EUA **não possuem um formato estabelecido**, mas devem incluir, no mínimo, relatórios traduzidos aplicáveis às Necessidades de Inteligência (NI) e uma avaliação da fonte da informação (Estados Unidos, 2017, tradução nossa, grifo nosso).

No que tange ao atendimento do princípio da oportunidade[6], a doutrina norte-americana determina que os comandantes devem receber informações de combate e produtos de Inteligência **em tempo hábil** e **em formato apropriado** para facilitar a

[6] O conhecimento de Inteligência deve ser produzido em prazo que assegure sua utilização completa e adequada, contribuindo diretamente para potencializar a capacidade do comandante de observar, orientar-se, decidir e agir (Brasil, 2015) .

consciência situacional e apoiar a tomada de decisões. A disseminação oportuna de informações é crítica para o sucesso das operações. A divulgação eficaz é deliberada e garante que os consumidores recebam a informação de que necessitam para conduzir as operações (Estados Unidos, 2017, tradução nossa, grifo nosso).

No Exército dos EUA, a doutrina de OSINT estabelece que há vários métodos e técnicas para disseminar o conhecimento produzido, dependendo da situação particular da missão e dos procedimentos operacionais padrão de cada Unidade, observadas as diretrizes da força conjunta. Esses métodos e técnicas de divulgação incluem a divulgação eletrônica direta (um programa/aplicativo de mensagens); mensagem instantânea; publicação na Web (com procedimentos de notificação para usuários); gravação de informações em mídia removível e enviá-las por meio de um serviço de correio seguro; gravação de informações em mídia removível e envio por meio eletrônico; e envio de documentos impressos por correio ou fax (Estados Unidos, 2017, tradução nossa).

No Comando de Inteligência das Forças Canadenses, prioriza-se a disseminação dos **Resumos Diários de OSINT** (OSINT Daily Summaries[7]) em meios não classificados, possibilitando amplo compartilhamento por e-mail ou qualquer sistema não classificado. Defende-se que este método de difusão garante aos usuários o acesso oportuno ao produto de OSINT em um dispositivo móvel**,** em qualquer lugar do mundo e a qualquer hora (Holtz; Maxwell, 2022, tradução nossa, grifo nosso).

[7] Produto diário de OSINT, sem classificação, amplamente compartilhado por e-mail ou qualquer sistema não classificado, a cargo da Equipe de Apoio Operacional de OSINT do Comando das Forças Canadenses – CFINTCOM OSINT Operational Support Team (Holtz; Maxwell, 2022, tradução nossa).

3 SITUAÇÃO ATUAL DA OSINT NO SISTEMA DE INTELIGÊNCIA DO EXÉRCITO

A decomposição da atual situação da OSINT no SIEx será realizada por intermédio da metodologia de fatores determinantes da capacidade, consubstanciadas pelo acrônimo DOPEMAI (doutrina, organização, pessoal, educação, material, adestramento e infraestrutura), conforme preconiza o Manual de Fundamentos Conceito Operacional do Exército Brasileiro – Operações de Convergência 2040 – EB20-MF-07.101 (Brasil, 2023b).

3.1 SITUAÇÃO ATUAL DO “DOPEMAI” DA OSINT NO SIEx

3.1.1 Doutrina

Atualmente, há uma lacuna de conhecimento sobre a Disciplina de Inteligência OSINT, no âmbito do SIEx. Os únicos aspectos doutrinários sobre a OSINT são abordados no Manual de Fundamentos Inteligência Militar Terrestre – EB20-MF-10.107 (Brasil, 2015), conforme se lê:

> 3.6.1 A Inteligência de Fontes Abertas (Open Source Intelligence - **OSINT**) é a Inteligência baseada em informações coletadas de fontes de caráter público, tais como os meios de comunicação (rádio, televisão e jornais), propaganda de estado, periódicos técnicos, internet, manuais técnicos e livros.
> 3.6.2 Os produtos OSINT **reduzem as demandas às outras disciplinas de Inteligência**, de maneira que essas se dediquem somente a obter dados que não possam ser adquiridos pelas fontes abertas.
> 3.6.3 Os **Órgãos de Inteligência devem conhecer a fundo as fontes abertas disponíveis**: quais são elas, sua confiabilidade e validade, como acessá-las etc.
> 3.6.4 A comunidade de Inteligência sempre usou fontes abertas na produção de conhecimento. A legislação sobre o acesso à informação produzida por órgãos públicos, ao redor do mundo, possibilita a obtenção de dados e informações sensíveis de Estados, organizações e instituições, o que é facilitado pela internet. **A OSINT é a fonte básica de Inteligência**. (Brasil, 2015, grifo nosso).

Em que pese a doutrina vigente abranger aspectos atuais sobre a OSINT, verifica-se que o conceito constante do manual é genérico, particularmente, ao se referir às “informações coletadas de caráter público da internet”, em comparação às doutrinas atualizadas dos Estados Unidos e do Reino Unido, por exemplo.

Considerando outros aspectos sobre a OSINT abordados no SIEx, resta clara a diferenciação entre a **fonte aberta disponível** e a **fonte protegida**. O Manual de Campanha EB70-MC-10.307 – Planejamento e Emprego da Inteligência Militar – estabelece que as **fontes protegidas** são aquelas cujos dados não estão disponíveis a qualquer pessoa, normalmente necessitando de técnicas apropriadas para que se

tenha acesso a eles, e que o fato de um dado não estar protegido não significa que ele esteja disponível. Com isso, a obtenção desses dados é realizada por operações de Inteligência, por intermédio de ações de **busca** (Brasil, 2016, grifo nosso).

Conforme o Manual de Campanha EB70-MC-10.232 – Guerra Cibernética – os **dados protegidos**, no espaço cibernético[8], são obtidos pelo especialista em Guerra Cibernética (G Ciber), por meio de ações de **coleta e de busca** (Brasil, 2017, grifo nosso). Nesse alinhamento, a doutrina do Manual de Fundamentos Inteligência Militar Terrestre – EB20-MF-10.107 estabelece que Inteligência Cibernética (Cyber Intelligence - CYBINT) é a Inteligência elaborada a partir de dados, **protegidos ou não**, obtidos no espaço cibernético (Brasil, 2015, grifo nosso).

Quanto à difusão de “produtos de OSINT” no SIEx, Oliveira (2023) ressaltou que algumas Agências de Inteligência do Brasil realizam a difusão de produtos não classificados, em forma de Resenha Crítica (RC) e Tema Crítico (TC), de acordo com o grau de relevância da temática, difundindo-os em canais personalizados de transmissão, com foco nos princípios da oportunidade e da necessidade de conhecer.

De acordo com o Plano de Desenvolvimento da Doutrina Militar Terrestre – PDDMT 2024 (Brasil, 2023a) – consta na Tabela 4 do Anexo B a previsão de difusão do Manual Técnico Inteligência de Fontes Abertas (EB70-MT-10.XXX), ainda em 2024.

No Brasil, a Lei Geral de Proteção de Dados (LGPD[9]) limita as ações de coleta de dados pessoais, quando tratados em desacordo com o que prescreve a lei (Brasil, 2018b).

3.1.2 Organização

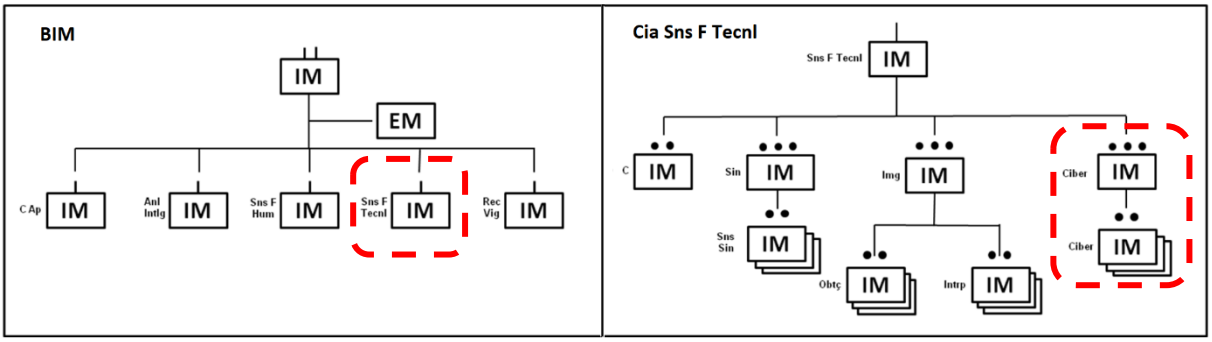
Até o momento, não há uma organização prevista para a OSINT no SIEx. No nível tático, o Batalhão de Inteligência Militar (BIM) possui, em sua estrutura organizacional, uma Companhia de Sensores de Fontes Tecnológicas (Cia Sns F Tecnl). No entanto, tal Subunidade não possui uma fração de OSINT (Brasil, 2018a).

---

[8] Espaço virtual composto por dispositivos computacionais conectados em rede, onde informações digitais trafegam, são processadas ou armazenadas (Brasil, 2015).

[9] Lei Nº 13.709, de 14 AGO 18 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Figura 3 – Organograma do BIM e da Cia Sns F Tecnl do BIM

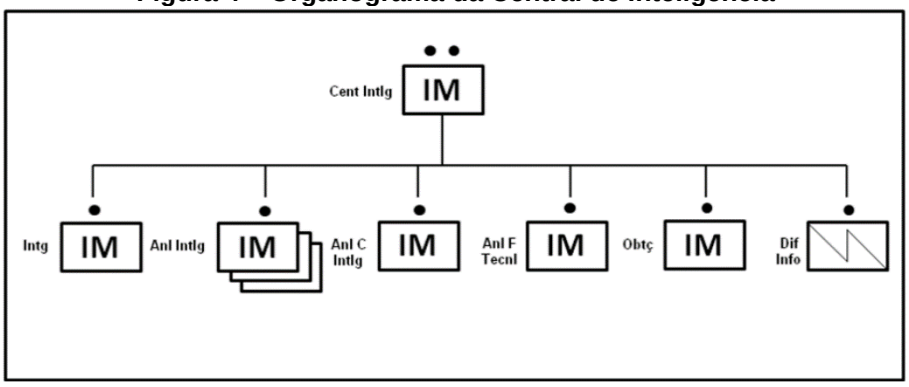


Fonte: Brasil (2018a), adaptado pelo autor.

No que concerne ao Fluxo de Inteligência nas operações, verifica-se que tanto na Célula de Análise da Central de Inteligência (Ambiente de Análise) como na Célula de Inteligência do Centro de Coordenação de Operações (CCOp) do escalão apoiado (Ambiente de Comando e Controle) – frações desdobradas pelo BIM – a obtenção de dados de OSINT é uma responsabilidade comum a “todas as turmas integrantes da Célula de Análise (Cel Anl)”, inexistindo elementos especializados em OSINT nessas estruturas (Brasil, 2018a).

Com relação ao Fluxo de Informações na Central de Inteligência (Cent Intlg), o Manual do BIM (Brasil, 2018a) estabelece que a Cent Intlg, em sua estrutura, deve contar com a participação de especialistas de todas as fontes de dados utilizadas na operação. No entanto, consta do mesmo manual, no item 3.4.8.5 que “a Turma de Análise de Fontes Tecnológicas (Tu Anl F Tecnl), da Cel Anl Intlg (da Central de Inteligência), é responsável por analisar dados técnicos provenientes das Fontes de Imagem, de Sinais e Cibernéticas recebidas”, verificando-se, assim, ausência de ligação com elementos especializados em OSINT nessa estrutura organizacional, conforme pode-se observar na Figura 4 (Brasil, 2018a).

Figura 4 – Organograma da Central de Inteligência



Fonte: Brasil (2018a).

3.1.3 Pessoal

No âmbito do SIEx, não há pessoal especializado, exclusivamente, em OSINT. Por esta razão, não há cargo específico nas AI para militares especialistas em Inteligência de Fontes Abertas.

3.1.4 Educação

Todos os cursos e estágios da Escola de Inteligência Militar do Exército (EsIMEx) contemplam carga horária de OSINT, de forma introdutória, apresentando a disciplina aos diversos instruendos. No entanto, não existe curso/estágio/capacitação específica de OSINT**,** na grade de especialização da Escola.

3.1.5 Material

Atualmente, as Agências de Inteligência (AI) do SIEx empregam seus meios orgânicos para a realização de ações de coleta em fontes abertas. É possível, porém, que algumas AI demandem por meios de tecnologia da informação e comunicações (MTIC), para suportar a estruturação de uma eventual fração de OSINT na AI.

3.1.6 Adestramento

Até o momento, não há Planos de Adestramento que contemplem a OSINT, no âmbito do SIEx. Contudo, sabe-se que militares do EB têm participado de seminários, oficinas e ciclos de palestras sobre OSINT, que são oferecidas com frequência por órgãos públicos e privados.

3.1.7 Infraestrutura

Nas condições atuais das AI do SIEx, o fator infraestrutura não se configura um problema substancial para a implementação da Disciplina de Inteligência de Fontes Abertas. Eventualmente, pode ser que algumas AI demandem por melhorias de infraestrutura de Tecnologia da Informação, com destaque para redes e serviços de internet.

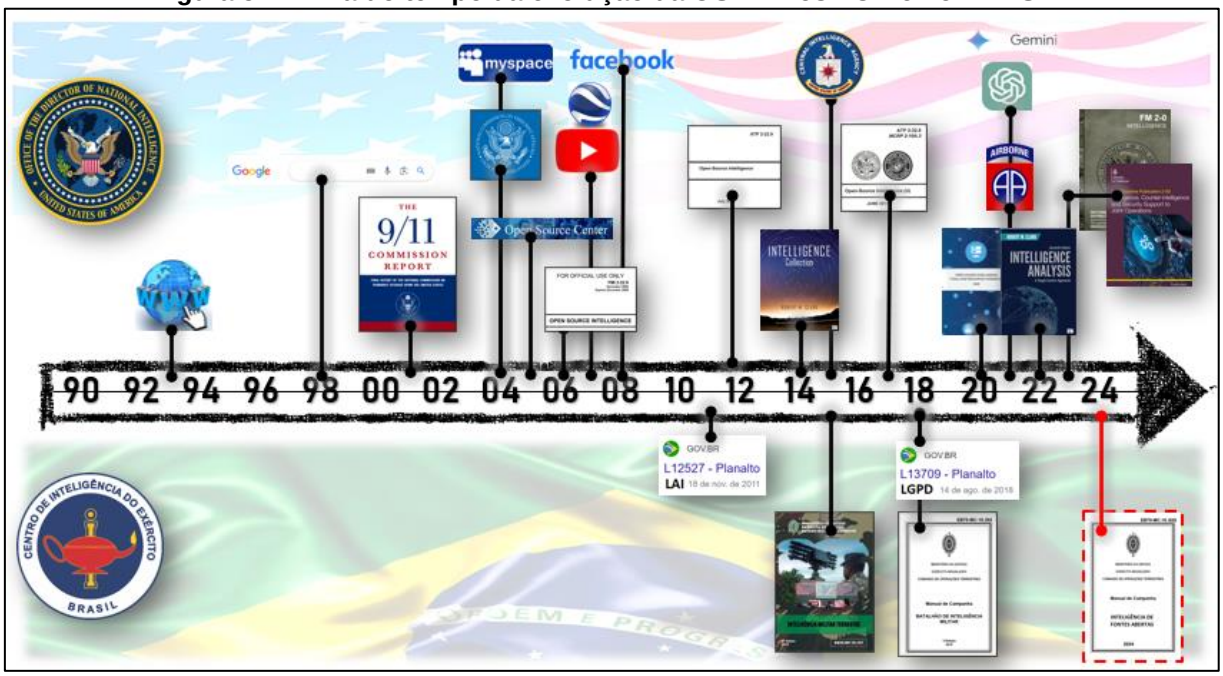
4 DISCUSSÃO

Nos capítulos anteriores, foram abordados os aspectos sobre a importância e as peculiaridades da OSINT, bem como a atual situação do emprego dessa Disciplina de Inteligência, no âmbito do SIEx. Com isso, buscou-se estudar os parâmetros adequados para sustentar uma proposta de estruturação da OSINT para o SIEx, objetivo geral do presente trabalho.

O estudo da história recente da OSINT, por intermédio da Técnica de Análise Estruturada (TAE) – Linha do Tempo, remete ao surgimento da internet, em 1993. Nos Estados Unidos, a OSINT se consolidou como fonte crucial de dados em prol da Segurança Nacional, após os ataques de 11 de setembro de 2001, expandindo sua influência com o avanço das redes sociais, nos anos seguintes. Em 2006, o Exército dos Estados Unidos lançou a versão inicial do Manual de OSINT – ATP 2-22.9, revisando-o constantemente com o apoio de experimentação em operações reais e de obras acadêmicas, com destaque para os livros do Dr. Robert M. Clark.

No Brasil, a OSINT ainda está em desenvolvimento, com estruturação incipiente nos órgãos governamentais, em comparação aos EUA. No SIEx, a estruturação da OSINT foi iniciada em 2015, com a publicação do Manual de Fundamentos Inteligência Militar Terrestre (EB20-MF-10.107). Desde então, o Exército Brasileiro vem estudando a implementação da Disciplina de Inteligência, no contexto da modernização da Doutrina Militar Terrestre brasileira.

Figura 5 – Linha do tempo da evolução da OSINT nos EUA e no BRASIL



Fonte: o autor.

Baseado no estudo até então apresentado, foi difundido um questionário (APÊNDICE A) para um universo de Analistas e Auxiliares de Analista de Inteligência, no período de 11 a 19 de maio de 2024, com 10 (dez) perguntas de múltipla escolha, a fim de colher suas opiniões quanto à estruturação da OSINT no SIEx, com foco nos aspectos do “DOPEMAI”.

4.1 OPINIÃO DOS ESPECIALISTAS

O questionário foi respondido por 43 militares que, atualmente, desempenham as funções de Analista de Inteligência/Auxiliar de Analista do SIEx, Chefes de Agência de Inteligência ou Comandantes de Batalhão de Inteligência Militar do Exército Brasileiro. Dentre as respostas recebidas, verificou-se que **65,1%** são de militares que **possuem o Curso Avançado de Inteligência**, da EsIMEx, fato que aumenta a relevância às respostas obtidas no questionário (grifo nosso).

Nos itens que se seguem, serão exploradas as respostas aos demais itens do questionário, de acordo com os fatores determinantes da capacidade (DOPEMAI) da OSINT.

4.1.1 Doutrina

A primeira questão versou sobre a relação custo/benefício no **esforço de obtenção**, no Ciclo de Inteligência. Das respostas, **97,7%** acreditam que o esforço de coleta/busca (NI) deve ser iniciado pela fonte mais barata e de fácil acesso, e que apenas as NI cujos dados são protegidos ou não obtidos em fontes abertas serão direcionados às fontes caras, que buscarão os dados protegidos (grifo nosso).

O próximo item buscou levantar a opinião dos especialistas acerca das capacidades de **atuação do analista de OSINT**. Como resultado, **95,3%** acreditam que é desejável que a OSINT seja realizada por um militar especialmente adestrado em OSINT, apto a empregar ferramentas, TTP de coleta, perito na identificação de vieses e táticas de engano (desinformação, dissimulação, fake news, etc.), com habilidade para navegar de forma anonimizada na Surface web, Deep Web e na Dark Web, tudo isso no contexto da chamada “Era da Informação” (Big data) (grifo nosso).

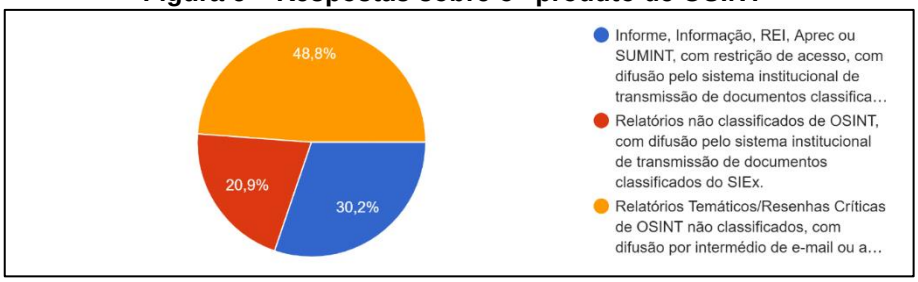
O item abaixo abordou a situação da implementação de “**produtos de OSINT**” no SIEx, seguindo o padrão de outros Exércitos, como o dos Estados Unidos, do Canadá e o da Austrália. O resultado foi que **48,8%** dos especialistas acreditam que esse processo deve funcionar com a implementação de Relatórios Temáticos/Resenhas Críticas de OSINT não classificados, com difusão por intermédio

de e-mail ou aplicativos de mensageria institucionais/institucionalizados, no âmbito do SIEx, cabendo compartilhamento no âmbito do SISBIN, com texto de redação livre, permitidas variações em sua forma e conteúdo, de acordo com as necessidades do cliente (grifo nosso).

As demais respostas do questão sobre os produtos de OSINT ficaram divididas em dois grupos: **30,2%** acreditam que o processo deve ser por intermédio de documentos de Inteligência (Infe, Info, REI, Aprec ou SUMINT) com restrição de acesso e com difusão pelo sistema institucional de transmissão de documentos classificados do SIEx; **20,9%** acreditam que deve ocorrer por meio de Relatórios não classificados de OSINT, mas com difusão pelo sistema institucional de transmissão de documentos classificados do SIEx (grifo nosso).

À luz da doutrina estudada até o momento, os dois últimos grupos de respostas mostraram-se **incompatíveis** com as características do conhecimento de OSINT, com destaque para o atendimento ao princípio da oportunidade, facilidade de transmissão, facilidade de acesso pelo decisor e a possibilidade de amplo compartilhamento no seio da Comunidade de Inteligência (grifo nosso).

Figura 6 – Respostas sobre o "produto de OSINT"

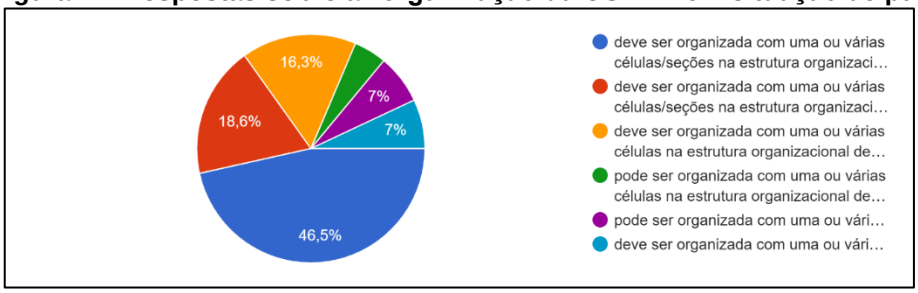


Fonte: o autor.

4.1.2 Organização

O quesito abaixo versou sobre a **organização da OSINT em situação de paz/normalidade institucional**, com destaque para a organização de "**células de OSINT**" nas AI. Nesse caso, a opinião majoritária dos especialistas (**46,5%**) apontou que a OSINT deve ser organizada com uma ou várias células/seções na estrutura organizacional da Agência Central do SIEx e nas agências Classe A e Especial (exceto Aditâncias). Nas AI Classe B, a célula de OSINT pode ser organizada, não sendo o caso a organização de célula de OSINT nas AI Classe C (grifo nosso).

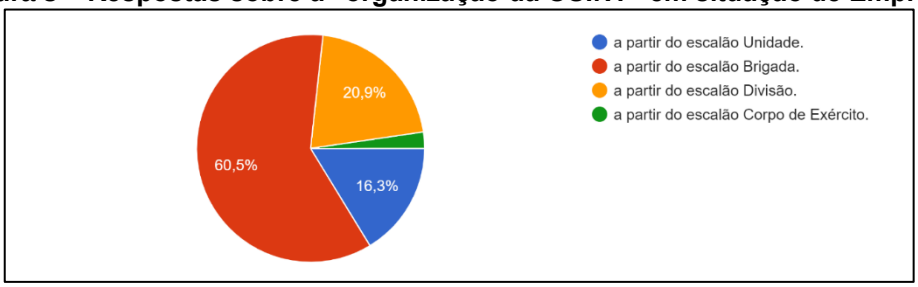
Figura 7 – Respostas sobre a "organização da OSINT" em situação de paz



Fonte: o autor.

De forma análoga, a próxima pergunta versou sobre a **organização da OSINT em situação de emprego (guerra ou não guerra)**. A grande maioria das respostas (**60,5%**) indicou que a OSINT deve ser organizada com, no mínimo, 1 (uma) células de OSINT, a partir do Escalão Brigada. Nesse caso, a revisão de literatura permite inferir que pode ser organizada uma célula de OSINT no escalão Unidade, dependendo sobremaneira dos fatores da decisão (grifo nosso).

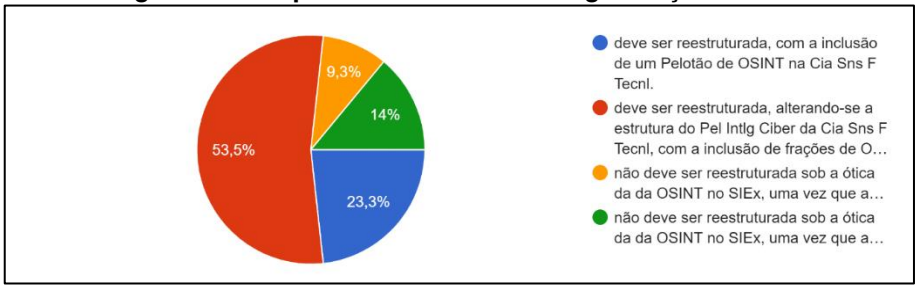
Figura 8 – Respostas sobre a "organização da OSINT" em situação de Emprego



Fonte: o autor.

Prosseguindo no questionário, formulou-se uma pergunta sobre as **lacunas de organização da OSINT na estrutura organizacional do BIM**, particularmente, quanto à ausência de frações de OSINT na Cia Sns F Tecnl. Como resposta, mais da metade dos especialistas (**53,5%**) acreditam que a estrutura organizacional do BIM deve ser reestruturada, alterando-se a organização do Pel Intlg Ciber da Cia Sns F Tecnl, com a inclusão de frações de OSINT nesse Pelotão.

Figura 9 – Respostas sobre a atual organização do BIM

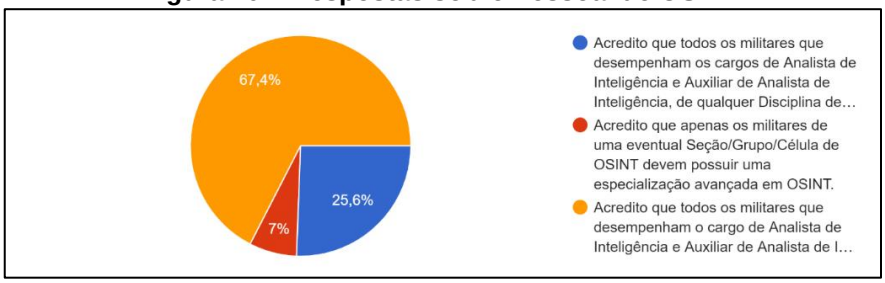


Fonte: o autor.

4.1.3 Pessoal

A questão relacionada ao pessoal buscou levantar as opiniões dos especialistas sobre quais militares devem ser especializados em OSINT. De forma majoritária, **67,4%** das respostas indicam que <u>todos os militares que desempenham o cargo de Analista de Inteligência e Auxiliar de Analista de Inteligência, de qualquer Disciplina de Inteligência, devem possuir uma especialização básica em OSINT, e que os militares de uma eventual Seção/Grupo/Célula de OSINT devem possuir uma especialização avançada em OSINT</u> (grifo nosso).

Figura 10 – Respostas sobre Pessoal de OSINT

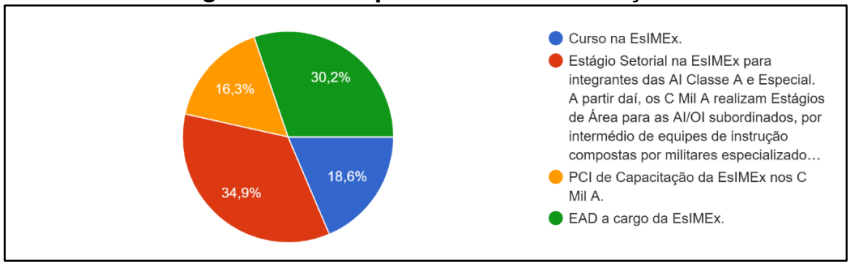


Fonte: o autor.

4.1.4 Educação

O item a seguir, relacionado à educação, apresentou respostas equilibradas dentre os especialistas sobre **como o analista de OSINT deve ser especializado**. Embora a maioria (**34,9%**) tenha optado pelo <u>estágio setorial na EsIMEx para integrantes das AI Classe A e Especial, e estágios de área para as demais AI</u>, a falta de unanimidade nas respostas deste quesito indicam que as demais opções (Curso na EsIMEx e PCI da EsIMEx) não podem ser totalmente descartadas no processo de implementação da OSINT no SIEx. Quanto à modalidade à distância, é provável que o EAD não surte os mesmos efeitos da especialização presencial. Ressalta-se, ainda, que outras opções podem ser levantadas, a exemplo da inclusão da carga horária de OSINT (uma ou duas Semanas de Instrução) no Curso Avançado de Inteligência (grifo nosso).

Figura 11 – Respostas sobre Educação



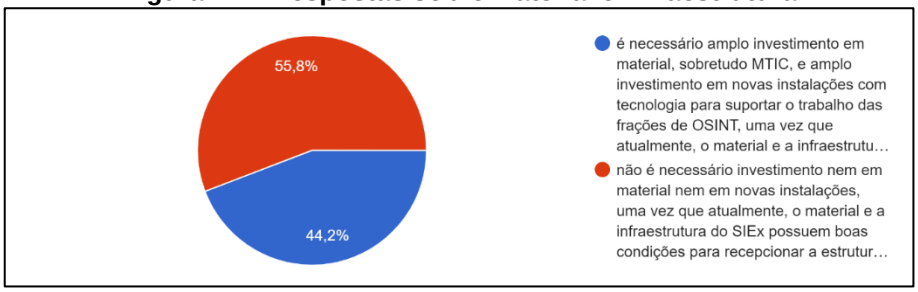
Fonte: o autor.

4.1.5 Perguntas relacionadas ao Material e à Infraestrutura

O último item do questionário versou sobre a necessidade de investimento em material e/ou infraestrutura, nas AI, de forma a melhor recepcionarem a estruturação da OSINT. O resultado foi equilibrado: **55,8%** dos analistas responderam que não é necessário investimento nem em material nem em novas instalações, uma vez que atualmente, o material e a infraestrutura do SIEx possuem boas condições para recepcionar a estruturação da OSINT, serão necessários apenas ajustes internos nas agências ; e 44,2% responderam o contrário, que é necessário amplo investimento em material e amplo investimento em novas instalações (grifo nosso).

Diante desse equilíbrio, avalia-se que é oportuno a flexibilização da situação em pauta, considerando que, eventualmente, algumas AI podem necessitar de investimentos pontuais, com destaque para a renovação do parque de computadores e de redes de TI em determinadas instalações.

Figura 12 – Respostas sobre Material e Infraestrutura



Fonte: o autor.

4.2 UMA PROPOSTA DE ESTRUTURAÇÃO DA OSINT PARA O SIEx

4.2.1 Doutrina

4.2.1.1 Atualização do conceito

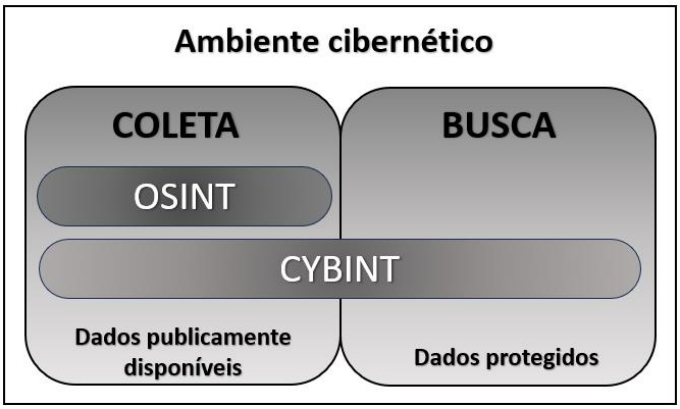
Inteligência de Fontes Abertas (OSINT) é a Inteligência produzida com base na coleta de informações oriundas de fontes abertas disponíveis, explorada e difundida em tempo hábil, com o objetivo de atender a uma ou várias necessidades de Inteligência.

As fontes abertas disponíveis são aquelas cujos dados são obtidos por meio ações de coleta, e incluem: todo o conteúdo online (*Surface Web, Deep Web e Dark Web*) disponível, normalmente, para qualquer pessoa; a mídia tradicional (jornais, revistas, rádio, televisão); publicações governamentais e não governamentais; redes sociais e outras plataformas de comunicação online; conteúdo gerado por usuários

em redes sociais (fotos, vídeos, comentários, wikis e blogs); informações disponibilizadas ao público em geral mediante solicitação e/ou pagamento; informações legalmente vistas ou ouvidas por qualquer observador casual ou disponibilizadas em uma reunião aberta ao público em geral; bancos de dados comerciais e acadêmicos; material em idioma estrangeiro disponível para o público em geral; material associações profissionais e acadêmico de conferências e simpósios; e outras informações não classificadas, como dados geoespaciais e imagens de satélite, informações financeiras e econômicas, registros públicos e documentos legais, metadados de arquivos digitais e transações financeiras.

As fontes protegidas são aquelas cujos dados não estão disponíveis a qualquer pessoa, necessitando de técnicas apropriadas para que se tenha acesso aos dados protegidos. O fato de um dado não estar protegido não significa que ele esteja disponível. No ambiente cibernético, a obtenção de dados protegidos é realizada por intermédio de ações de busca, a cargo da Inteligência Cibernética (CYBINT).

Figura 13 – Ações de Inteligência no ambiente cibernético



Fonte: o autor.

4.2.1.2 Tipos de coleta

a) Coleta passiva: é a coleta de informações que envolve métodos passivos, como leitura, observação ou monitoramento, sem necessidade de interação do coletor com a fonte.

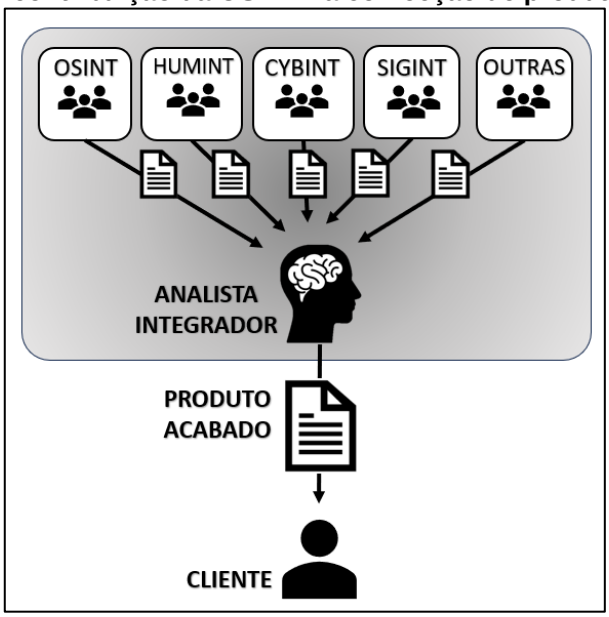
b) Coleta ativa: é a coleta de informações que envolve métodos ativos, como solicitação de informações, acesso (*login*), assinaturas, interação em redes sociais ou fóruns exclusivos, ou seja, métodos que exigem a interação do coletor com a fonte.

4.2.1.3 Finalidades da OSINT

a) Servir como fonte para a confecção de produtos de OSINT (fonte única) ou de “produtos acabados” de Inteligência (abordagem multidisciplinar).

b) Acionar, validar, ampliar e melhorar a coleta/busca realizada por outra Disciplina de Inteligência.

Figura 14 – A contribuição da OSINT na confecção de produtos acabados



Fonte: o autor.

4.2.1.4 Características da OSINT

a) A OSINT é a fonte básica de Inteligência.

b) É a fonte de maior disponibilidade e facilidade de coleta.

c) Necessita do emprego de táticas, técnicas e procedimentos (TTP) e ferramentas específicas para as ações de coleta de informações.

d) Os dados oriundos de fontes abertas disponíveis são, via de regra, acessíveis a qualquer pessoa.

e) As fontes abertas disponíveis possuem elevada volatilidade, exigindo um monitoramento contínuo e análise ágil para garantir a relevância e a oportunidade das informações coletadas.

f) Os produtos de OSINT, normalmente, não possuem restrição de acesso, e podem ser difundidos por intermédio de e-mail ou aplicativos de mensageria institucionais.

4.2.1.5 Capacidades da OSINT

a) Possibilitar a coleta de informações sobre uma vasta gama de assuntos, proporcionando uma visão abrangente de consciência situacional.

b) Funcionar como um sistema de processamentos de dados oriundos de fontes abertas, possibilitando a difusão de produtos de forma rápida e eficiente, em formato e meio de transmissão apropriados, permitindo respostas ágeis a eventos e ameaças emergentes.

c) Reduzir as demandas das outras disciplinas de Inteligência, de maneira que essas se dediquem somente a obter dados que não possam ser adquiridos pelas fontes abertas disponíveis.

d) Ampliar a capacidade de obtenção de consciência situacional, em todos os níveis, e fornecer atualizações de informações quase que em tempo real aos combatentes.

e) Integrar-se com outras disciplinas de Inteligência para garantir uma abordagem multidisciplinar.

f) Fortalecer as relações e o compartilhamento de informações com parceiros e aliados estrangeiros.

4.2.1.6 Vulnerabilidades da OSINT

a) Exposição a ações de negação, engano, desinformação, notícias falsas, dissimulação, ações psicológicas e fraude.

b) A coleta e análise de informações em fontes abertas podem expor os interesses e as intenções de uma organização, tornando-a vulnerável a contramedidas e ataques direcionados. É fundamental adotar medidas de segurança e privacidade para proteger as operações de OSINT.

c) Os dados coletados carecem da avaliação da fonte e do conteúdo, particularmente, quanto à precisão, credibilidade, autenticidade, sensibilidade, oportunidade e viés.

d) Os dados coletados em idioma estrangeiro podem conter regionalismos ou gírias.

e) A OSINT depende de ferramentas e tecnologias específicas, além de profissionais especialmente adestrados em OSINT.

4.2.1.7 Limitações da OSINT

a) O volume exponencial de informações publicamente disponíveis extrapola as capacidades humanas de localizar, coletar e processar informações relevantes, inclusive em idioma estrangeiro, sem o emprego de Meios de Tecnologia da Informação e Comunicações (MTIC) ou IA.

b) Algumas informações relevantes para a Inteligência Militar podem estar protegidas por medidas de segurança ou disponíveis apenas em fontes fechadas, limitando o escopo da OSINT.

c) A coleta e análise de informações na OSINT são realizadas dentro dos limites da lei, sem recorrer a métodos clandestinos ou ilegais, garantindo a legitimidade e a ética das operações.

4.2.1.8 Ciclo de processamento da OSINT

O ciclo de processamento da OSINT obedece às seguintes fases:

a) Planejamento – estudo do Plano de Obtenção do Conhecimento; confecção do Plano de Coleta, considerando os dados disponíveis em banco de dados e de informações em fontes abertas disponíveis.

b) Exploração – ações de coleta, integração com outras fontes, avaliação da fonte e do conteúdo, gerenciamento de risco, análise e produção de conhecimentos.

c) Difusão – transmissão de produtos de OSINT, compartilhamento de Inteligência acionável e monitoramento do alvo e do feedback do decisor.

Figura 15 – Ciclo de processamento da OSINT

Fonte: o autor.

4.2.1.9 Produtos de OSINT

Os produtos de OSINT são documentos de Inteligência que não possuem restrição de acesso. O texto é de redação livre, sendo permitidas variações em sua forma e conteúdo, de acordo com as necessidades do cliente. Normalmente, formalizam-se em Relatórios Temáticos, Temas Críticos, Resenhas Críticas, Resumos, Sumários ou Alertas.

- APÊNDICE B – Modelo de Relatório Temático.

- APÊNDICE C – Modelo de Resenha Crítica.

4.2.2 Organização

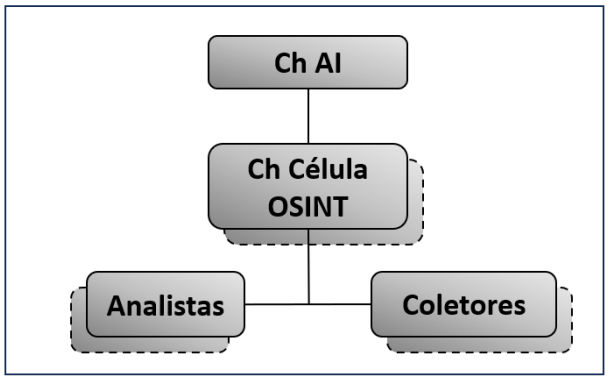
4.2.2.1 Estruturação organizacional da OSINT

a) Em situação de paz/normalidade institucional

1) Células de OSINT na estrutura organizacional da Agência Central do SIEx e nas agências Classe A e Especiais (exceto Aditâncias). Nas AI classes B e C, a limitação de meios pode ser um fator que inviabilize a constituição da célula de OSINT, fator que pode ser mitigado com a capacitação dos integrantes da agência, fomentando o compartilhamento de informações na cadeia de comando.

2) A organização da OSINT em células de Inteligência nas AI deve ser flexível, variando de acordo com a conjuntura, eixos temáticos[10] de acompanhamento e/ou requisitos do cliente.

Figura 16 – Célula de OSINT



Fonte: o autor.

3) Os integrantes da célula de OSINT realizam, normalmente, as tarefas descritas no quadro 1.

[10] Eixos temáticos de acompanhamento podem ser representados pelas variáveis operacionais (políticas, militares, económicas, sociais, de informação, infra-estruturas – PMESII – e pelas considerações civis (áreas, estruturas, capacidades, organizações, pessoas e eventos – AECOPE (Gack, 2023, tradução nossa).

Quadro 1 – Proposta de missões para os especialistas em OSINT

Função	Missões
Chefe da célula de OSINT	Coordenar o trabalho de obtenção da equipe; priorizar e supervisionar a execução do Plano de Coleta de OSINT; ligar-se com outras agências da Comunidade de Inteligência de OSINT (compartilhamento); aprovar os produtos internos de OSINT; monitorar o apoio contínuo de Inteligência à AI enquadrante; providenciar o recebimento e a difusão de produtos OSINT.
Analista de OSINT	Integrar, traduzir, analisar e produzir conhecimentos de OSINT; supervisionar as atividades de contrainteligência; gerenciar o risco envolvido na produção de OSINT; assessorar o Ch Cel OSINT na confecção e supervisão do Plano de Coleta de OSINT.
Coletor OSINT	Monitorar o ambiente cibernético em busca de informações publicamente disponíveis e relevantes para a consciência situacional; gerenciar o banco de dados da célula; realizar a coleta de dados em fontes abertas; e realizar a avaliação da fonte e do conteúdo dos dados coletados.

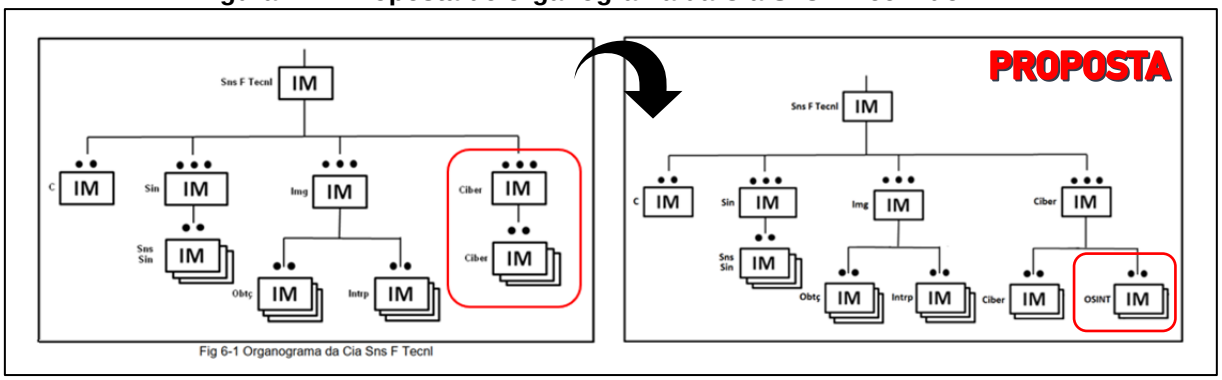
Fonte: o autor.

b) Em situação de emprego, guerra ou não guerra:

1) No Ambiente de Comando e Controle: 1 (uma) ou várias turmas temáticas de OSINT, de composição flexível, de acordo com os fatores da decisão[11], na Célula de Inteligência do Centro de Coordenação das Operações (CCOp) do escalão apoiado.

2) No Ambiente de Obtenção: 2 (dois) Grupos de OSINT no Pelotão de Inteligência Cibernética da Companhia de Sensores de Fontes Tecnológicas (Cia Sns F Tecnl) do BIM.

Figura 17 – Proposta de organograma da Cia Sns F Tecnl do BIM



Fonte: Brasil (2018a), adaptado pelo autor.

3) No Ambiente de Análise: a Central de Inteligência, em sua estrutura, deve contar com a participação de especialistas de todas as fontes de dados utilizadas na operação; a Turma de Análise de Fontes Tecnológicas, da Célula de Análise de

[11] Elementos que orientarão o processo decisório. Os principais fatores da decisão são: missão, inimigo, terreno e condições meteorológicas, meios, tempo e considerações civis (Manual de Campanha EB70-MC-10.223 Operações, 5ª Edição, 2017).

Inteligência da Central de Inteligência é responsável por analisar dados técnicos provenientes de fontes abertas, de imagem, de sinais e cibernéticas recebidas.

4.2.3 Pessoal

Com relação aos levantamentos de aspectos relacionados ao Pessoal do SIEx, sob a ótica da estruturação da OSINT, o presente estudo não visualiza incrementos em termos de criação de claros nos Quadros de Claros de Pessoal das AI. Trata-se, na verdade, de amplas medidas de capacitação do pessoal orgânico que desempenha as funções de Analistas de Inteligência ou Auxiliares de Analista de Inteligência, qualificando-os ao desempenho das funções de analista/coletor das frações de OSINT, quando ativadas.

4.2.4 Educação

Com relação à educação, propõe-se que a especialização de militares em OSINT seja realizada por todos os militares que desempenham a função de Analistas de Inteligência ou Auxiliares de Analista de Inteligência, de qualquer Fonte de Inteligência.

Dito isto, visualiza-se que a formação do recurso humano especializado em OSINT deva ocorrer das seguintes formas, não excludentes entre si:

a) Estágio Setorial na EsIMEx para integrantes das AI Classes A e Especial;

b) Estágios de Área para as AI Classes B e C, por intermédio de equipes de instrução compostas por militares especializados na EsIMEx;

c) Pedido de Cooperação de Instrução (PCI) de Capacitação da EsIMEx junto aos C Mil A, para os integrantes das AI daquele comando; e

d) Inclusão da carga horária de 2 (duas) semanas de instrução na grade curricular dos cursos Avançado de Inteligência, e de 1 (uma) semana de instrução nos demais cursos regulares da EsIMEx.

4.2.5 Material

A estruturação da OSINT, no âmbito do SIEx, não acarreta na aquisição de material complementar, uma vez que as AI já empregam seus meios orgânicos para a realização da OSINT. No entanto, aventa-se a possibilidade de que algumas agências demandem por adequações de MTIC, particularmente, na renovação do parque de computadores ou aquisição de softwares especializados, por exemplo.

4.2.6 Adestramento

O adestramento dos integrantes das frações de OSINT das AI deve ser contínuo, com o objetivo de manter os militares atualizados com as últimas tendências e tecnologias da Inteligência de Fontes Abertas. Nesse sentido, é fundamental promover a troca de experiências e o intercâmbio de conhecimentos com outras instituições e agências de inteligência, nacionais e estrangeiras, para acompanhar o desenvolvimento da OSINT no âmbito da Comunidade de Inteligência mundial.

Dessa forma, visualiza-se que o adestramento em OSINT pode ser implementado por intermédio de:

a) Planos de Adestramento de OSINT, a cargo das AI; e

b) participação em seminários, workshops, oficinas e ciclos de palestras sobre OSINT, nos órgãos públicos e privados, nacionais e internacionais.

4.2.7 Infraestrutura

Da mesma forma que o material, a estruturação da OSINT, no âmbito do SIEx, não acarreta no investimento complementar em infraestrutura. Porém, visualiza-se que, eventualmente, algumas AI demandem por melhorias pontuais de infraestrutura de Tecnologia da Informação, com destaque para redes e serviços de internet ou implantação de servidores de rede dedicados, por exemplo.

5 CONCLUSÃO

Em face do exposto, o presente trabalho cumpriu o seu objetivo de propor um modelo de estruturação da Inteligência de Fontes Abertas (OSINT) no âmbito do SIEx. Para tanto, foram analisadas as peculiaridades da OSINT na Comunidade de Inteligência e a situação atual de seu emprego no SIEx, culminando em uma proposta de organização estrutural para a disciplina. Dessa forma, a pesquisa demonstrou o potencial da OSINT em aumentar a efetividade da produção de Inteligência acionável, contribuindo significativamente para o processo decisório das autoridades militares.

Um ponto de destaque nesse estudo foi a análise da evolução da OSINT, desde seu crescimento exponencial após os ataques de 11 de setembro nos EUA até sua recente incorporação na doutrina do Exército Brasileiro, em 2015. Logo, ressalta-se a necessidade de constante modernização da estrutura de Inteligência Militar para acompanhar a evolução da arte da guerra, no contexto mundial.

Diante disso, a pesquisa corrobora a visão de que a OSINT não deve ser encarada como mera ferramenta, mas sim como uma disciplina de Inteligência equiparável às demais, uma vez que 80% dos dados relevantes estao disponíveis em fontes abertas, conforme estimado por especialistas no tema.

Ademais, o levantamento da situação atual da OSINT no SIEx revelou uma lacuna doutrinária sobre o tema, o que pode acarretar em dificuldades na coleta, análise e disseminação de dados relevantes para a produção de conhecimento de Inteligência. A falta de padronização e de procedimentos claros pode comprometer a eficiência e a eficácia da OSINT, impactando diretamente a Metodologia de Produção do Conhecimento do Exército Brasileiro.

Outro ponto de destaque é que as opiniões dos especialistas consultados por intermédio de questionário corroboram os aspectos levantados no trabalho e as propostas de estruturação da OSINT no SIEx, conferindo relevância e oportunidade ao estudo. A convergência de visões entre a pesquisa bibliográfica e a opinião dos especialistas fortalece a necessidade de uma abordagem integrada e multidisciplinar para a produção de Inteligência, na qual a OSINT desempenha um papel central.

Assim, pode-se inferir que o compartilhamento de produtos de OSINT na Comunidade de Inteligência é uma tendência mundial, fundamental para garantir a disseminação oportuna e eficiente de conhecimentos de Inteligência. A utilização de

softwares especializados, aliada ao crescente emprego de IA, também se mostra promissora para o aprimoramento da OSINT no SIEx.

Pode-se concluir, ainda, que a OSINT, por suas características, apresenta-se como uma disciplina singular. A natureza das fontes abertas disponíveis e a legalidade de seus métodos a tornam acessível e de baixo custo, permitindo uma coleta ágil e abrangente de informações. Sua capacidade de complementar outras disciplinas de Inteligência, como HUMINT, SIGINT e IMINT, a torna ainda mais valiosa para a produção do conhecimento, com destaque para o nível tático.

Em contrapartida, a OSINT também enfrenta desafios. A primordial necessidade de avaliação da fonte e do conteúdo, o extenso volume de informações e a manipulação da verdade, configuram limitações que exigem constante treinamento e o desenvolvimento de técnicas e ferramentas especializadas para superá-las. A vulnerabilidade às ações de negação e engano, aliada à dependência tecnológica inerentes à disciplina, também são aspectos que demandam constante aprimoramento das ações de coleta de OSINT.

Em que pese este trabalho não esgotar o assunto, serve como um ponto de partida sólido para a estruturação do “DOPEMAI” da OSINT no SIEx, além de contribuir para a revisão de outros produtos doutrinários da Força. A estudo contínuo e o aperfeiçoamento dessa estrutura são essenciais para garantir sua efetividade e relevância para a Inteligência Militar.

Nesse sentido, sugere-se, como temas para trabalhos futuros sobre a OSINT, o aprofundamento da pesquisa sobre o uso de IA na análise de dados de fontes abertas disponíveis, bem como investigar o desenvolvimento de ferramentas e técnicas específicas de OSINT no Processo de Planejamento e Condução das Operações Terrestres (PPCOT).

Por fim, espera-se que este trabalho contribua para a evolução da Doutrina de Inteligência Militar Terrestre, ao identificar e propor soluções para as lacunas existentes na estruturação da OSINT, no âmbito do SIEx. Espera-se, ainda, que a implementação das propostas apresentadas neste estudo resulte no aumento da efetividade das operações militares, em face do aprimoramento da produção de conhecimento de Inteligência, com reflexos positivos para o processo decisório, em todos os níveis, no Exército Brasileiro.

REFERÊNCIAS

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. **Manual Técnico Produção do Conhecimento de Inteligência – EB70-MT-10.401**. 1ª ed. Brasília, DF, 2019.

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. **Manual de Campanha Planejamento e Emprego da Inteligência Militar – EB70-MC-10.307**. 1ª ed. Brasília, DF, 2016.

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. **Manual de Campanha Guerra Cibernética – EB70-MC-10.232**. 1ª ed. Brasília, DF, 2017.

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. **Manual de Campanha Batalhão de Inteligência Militar – EB70-MC-10.302**. 1ª ed. Brasília, DF, 2018a.

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. **Plano de Desenvolvimento da Doutrina Militar Terrestre – PDDMT – EB70-P-10.001**. Edição 2024. Brasília, DF, 2023a.

BRASIL. Exército Brasileiro. Estado-Maior do Exército. **Manual de Fundamentos Inteligência Militar Terrestre (EB20-MF-10.107)**. 2ª ed. 2015.

BRASIL. Exército Brasileiro. Estado-Maior do Exército. **Manual de Fundamentos Conceito Operacional do Exército Brasileiro – Operações de Convergência 2040 (EB20-MF-07.101)**. 1ª ed. 2023b.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/ lei/l13709.htm. Acesso em: 26 maio 2024.

CLARK, Robert M. **Intelligence analysis:** A Target Centric Approach. 7. ed. Washington, D.C.: CQ Press, 2022.

CLARK, Robert M. **Intelligence collection**. Washington, D.C.: CQ Press, 2014.

CLARK, Robert M.; MITCHELL, William L. **Deception, Counterdeception and Counterintelligence**. Washington, D.C.: CQ Press, 2019.

ESTADOS UNIDOS. Headquarters, Department of the Army. **FM 2-0 Intelligence**. Washington, DC: U.S. Government Printing Office, 2023. Disponível em: https://irp.fas.org/doddir/army/fm2_0.pdf. Acesso em: 26 abr. 2024.

ESTADOS UNIDOS. Headquarters, Department of the Army. **ATP 2-22.9 Open-Source Intelligence**. Washington, DC: U.S. Government Printing Office, 2017. Disponível em: https://irp.fas.org/doddir/army/atp2-22-9-2017.pdf. Acesso em: 26 abr. 2024.

GACK, Jay. The Open-Source Intelligence conundrum: creating the discipline or integrating the data? **Military Intelligence Professional Bulletin**. Fort Huachuca, v. 34, n. 2, p. 17-22, Apr. 2022. Disponível em: https://irp.fas.org/agency/army/mipb/2022_01.pdf. Acesso em: 22 abr. 2024.

GEIGER, Corrine. The reawakening of Open-Source Intelligence. **Military Intelligence Professional Bulletin**, Fort Huachuca, v. 34, n. 2, p. 9-12, Apr. 2022. Disponível em: https://irp.fas.org/agency/army/mipb/2022_01.pdf. Acesso em: 22 abr. 2024.

HOLTZ, David; MAXWELL, Angela. Open-Source Intelligence in the Canadian Intelligence Community. **Military Intelligence Professional Bulletin**. Fort Huachuca, v. 34, n. 2, p. 13-16, Apr. 2022. Disponível em: https://irp.fas.org/agency/army/mipb/2022_01.pdf. Acesso em: 22 abr. 2024.

HOPPER, Greg. Open-Source Intelligence: developing analytical capability for the Australian Army. **Military Intelligence Professional Bulletin**. Fort Huachuca, v. 34, n. 2, p. 23-26, Apr. 2022. Disponível em: https://irp.fas.org/agency/army/mipb/2022_01.pdf. Acesso em: 22 abr. 2024.

LE DEUFF, Olivier. L'Open Source Intelligence (OSINT): origine, définitions et portée, entre convergence professionnelle et accessibilité à l'information. **I2D - Information, données & documents**, vol. 1, no. 1, 2021, pp. 14-20. Disponível em: https://www.cairn.info/revue-i2d-information-donnees-et-documents-2021-1-page-14.htm. Acesso em: 26 maio 2024.

OLIVEIRA, Jorge Alfredo Henriques. **A produção do conhecimento de inteligência no Exército Brasileiro em face das necessidades de inteligência corrente e prospectiva**. 2023. Trabalho de Conclusão de Curso (Especialização em Análise de Inteligência) – Escola de Inteligência Militar do Exército, Brasília, 2023.

POTTER, Laura; BEMBENEK, Christina. The risk of not knowing: Enabling Intelligence Professionals to Leverage Publicly Avaliable Information. **Military Intelligence Professional Bulletin**, Fort Huachuca, v. 34, n. 2, p. 5-8, Apr. 2022. Disponível em: https://irp.fas.org/agency/army/mipb/2022_01.pdf. Acesso em: 22 abr. 2024.

REINO UNIDO. Ministry of Defence. **JDP 2-00 Intelligence, Counter-intelligence and Security Support to Joint Operations**. 4ª ed. Shrivenham: Defence Academy of the United Kingdom, 2023. Disponível em: https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf. Acesso em: 26 abr. 2024.

APÊNDICE A - QUESTIONÁRIO

A ESTRUTURAÇÃO DA OSINT, COMO DISCIPLINA DE INTELIGÊNCIA, NO ÂMBITO DO SIEx.

*(Tempo de resposta estimado em 10 min)

Olá!

Sou o Ten Cel Inf Celso Augusto Carvalho SAMPAIO e solicito seu apoio por meio do preenchimento deste questionário como parte do Trabalho de Pós-graduação Lato Sensu de Especialização em Análise de Inteligência.

Atualmente, sou aluno do Curso Avançado de Inteligência da EsIMEx e estou desenvolvendo um Trabalho de Conclusão de Curso (TCC) com o tema "**A ESTRUTURAÇÃO DA OSINT, COMO DISCIPLINA DE INTELIGÊNCIA, NO ÂMBITO DO SIEX**".

Meu trabalho visa ao preenchimento da lacuna da não estruturação dos fatores determinantes da capacidade da OSINT no SIEx (**DOPEMAI: doutrina, organização, pessoal, educação, material, adestramento e infraestrutura**), conforme preconiza o Manual de Fundamentos Conceito Operacional do Exército Brasileiro – Operações de Convergência 2040 (EB20-MF-07.101).

Desde já sou grato pela sua valiosa contribuição!

ANTES DE TUDO, INTELIGÊNCIA!

E-mail

_____

DOPEMAI

Considerações essenciais

✓Todas as perguntas referem-se ao SIEx.

✓A OSINT **NÃO ESTÁ ESTRUTURADA** no SIEx. Segundo o PDDMT/24, há a previsão de a previsão de difusão do Manual Técnico Inteligência de Fontes Abertas (EB70-MT-10.XXX), ainda em 2024.

✓A OSINT é a Fonte de Inteligência **DOMINANTE** para a maioria dos analistas. Nos ESTADOS UNIDOS, a quantidade de inteligência derivada de OSINT foi estimada em cerca de **80%** (Clark, 2022).

✓No âmbito das disciplinas tecnológicas de Inteligência, têm-se que a OSINT realiza SOMENTE ações de **coleta de dados**, enquanto a CIBYNT realiza a **coleta e a busca de dados**.

✓Marque apenas 1 resposta para cada pergunta.

O Senhor é

( ) Analista/Auxiliar de Inteligência possuidor do Curso Avançado de Inteligência.

( ) Analista/Auxiliar de Inteligência sem o Curso Avançado de Inteligência/EsIMEx.

DOUTRINA/ORGANIZAÇÃO/EDUCAÇAO/PESSOAL

Considerações para as perguntas de 1 a 4:

✓Sabe-se, no âmbito da Comunidade de Inteligência, que a OSINT é a de menor custo, quando comparada com HUMINT, SIGINT, IMINT e MASINT. Enquanto a primeira emprega TTPs para a COLETA de dados publicamente disponíveis, empregando meios da infraestrutura existente nas instituições, as demais envolvem custos logísticos e operacionais que variam de acordo com a missão,

para realizar ações de BUSCA de dados protegidos (ou não disponíveis ainda, no caso da IMINT e MASINT. - O recurso humano das fontes HUMINT, SIGINT, IMINT e MASINT é EXÍGUO, e as demandas por conhecimento de Inteligência são grandes.
✓A produção do conhecimento de Inteligência deve atender ao princípio da oportunidade, com o fim de MELHORAR o entendimento da situação pelos comandantes e, consequentemente, os seus processos decisórios.
✓A aplicação do PRINCÍPIO DA EFETIVIDADE (capacidade de se alcançar plenamente um objetivo utilizando o mínimo de recursos possível, de modo a cumprir com a finalidade definida e ainda assim se evitar desperdícios) permeia o emprego dos meios do SIEx.

1) Sobre a efetividade das ações de obtenção do conhecimento de Inteligência:
( ) Acredito que o esforço de coleta/busca (NI) deve ser iniciado pelas fontes mais caras, por que são as mais importantes e oferecem produtos de melhor qualidade. Em seguida, complementa-se o conhecimento com algum dado relevante oriundo de OSINT, finalizando a produção do conhecimento.
( ) Acredito que o esforço de coleta/busca (NI) deve ser iniciado pela fonte mais barata e de fácil acesso. Apenas as NI cujos dados são protegidos ou não obtidos em fontes abertas serão direcionados às fontes caras, que buscarão os dados protegidos.

2) Sobre o emprego da OSINT no Ciclo de Inteligência do SIEx:
( ) Acredito que qualquer militar com conhecimentos básicos em ferramentas de busca na internet, como google e similares, tem condições ideais para realizar ações de OSINT em proveito da AI, no desempenho da função de assessor de Inteligência.
( ) Acredito que é desejável que a OSINT seja realizada por um militar especialmente adestrado em OSINT, apto a empregar ferramentas, TTP de coleta, perito na identificação de vieses e táticas de engano (desinformação, dissimulação, fake news, etc.), com habilidade para navegar de forma anonimizada na surface web, Deep Web e na Dark Web, tudo isso no contexto da chamada "Era da Informação" (Big data).

3) No âmbito do SIEx, QUEM o Sr acha que deve possuir especialização em OSINT?
( ) Acredito que todos os militares que desempenham os cargos de Analista de Inteligência e Auxiliar de Analista de Inteligência, de qualquer Disciplina de Inteligência, devem possuir uma especialização básica em OSINT.
( ) Acredito que apenas os militares de uma eventual Seção/Grupo/Célula de OSINT devem possuir uma especialização avançada em OSINT.
( ) Acredito que todos os militares que desempenham o cargo de Analista de Inteligência e Auxiliar de Analista de Inteligência, de qualquer Disciplina de Inteligência, devem possuir uma especialização básica em OSINT, e que os militares de uma eventual Seção/Grupo/Célula de OSINT devem possuir uma especialização avançada em OSINT.

4) Coerente com a sua resposta no item anterior e considerando o fator custo- * benefício das linhas de ação apresentadas, COMO o Sr acredita que o analista de OSINT deve ser especializado?
( ) Curso na EsIMEx.
( ) Estágio Setorial na EsIMEx para integrantes das AI Classe A e Especial. A partir daí, os C Mil A realizam Estágios de Área para as AI/OI subordinados, por intermédio de equipes de instrução compostas por militares especializados na EsIMEx.
( ) PCI de Capacitação da EsIMEx nos C Mil A.
( ) EAD a cargo da EsIMEx.

5) No processo de estruturação da OSINT no SIEx, sob o enfoque de PESSOAL, o Sr acha que
( ) é necessário um aumento de claros de pessoal para o desempenho das funções de Analista de OSINT das novas frações de OSINT nas AI.
( ) não é necessário um aumento de claros de pessoal para o desempenho das funções de Analista de OSINT das novas frações de OSINT nas AI, mas sim uma reorganização interna associada ao adestramento das novas frações.

ORGANIZAÇÃO
Considerações para as perguntas 6 e 7:
✓A Doutrina de Defesa dos ESTADOS UNIDOS conta com células de OSINT nas seções de Inteligência, desde o escalão Brigada (Brigade Combat Team e Marine Air-Ground Task Force –

MAGTF). Na intenção de estruturar um modelo de organização da OSINT no SIEx, considerando as peculiaridades dos diversos tipos de organização de Inteligência (órgãos e agências) e as limitações do EB (pessoal e orçamento), as perguntas a seguir referem-se a COMO o Sr acredita que deve ser implantada a organização da OSINT no SIEx.

Exemplo de célula de OSINT na "Marine Air-Ground Task Force - MAGTF"

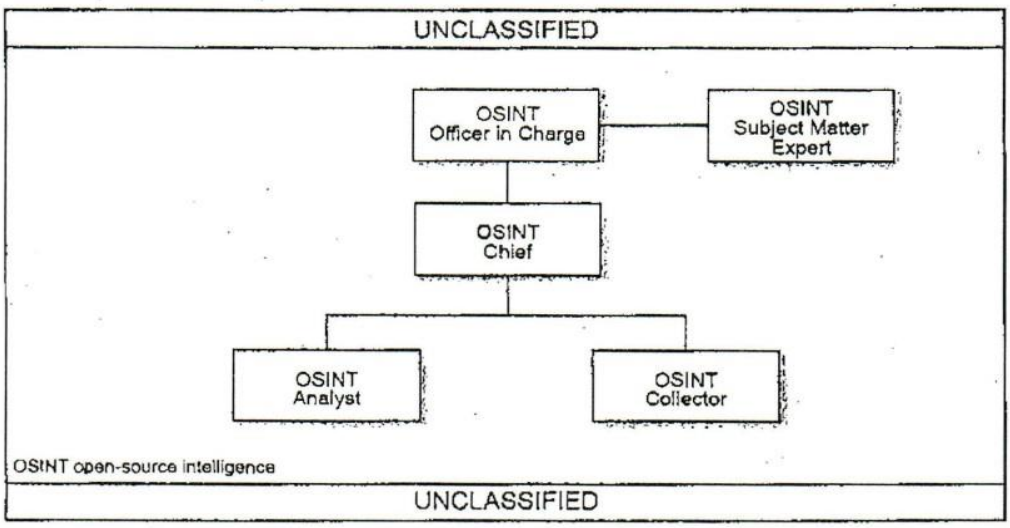


Figure 2-2. (U) *Marine-air ground task force intelligence center OSINT cell example*

6) Em situação de paz/normalidade institucional, a OSINT

( ) deve ser organizada com uma ou várias células/seções na estrutura organizacional da Agência Central do SIEx e nas agências Classe A e Especial (exceto Aditâncias). Nas AI Classe B, a célula de OSINT pode ser organizada, não sendo o caso a organização de célula de OSINT nas AI Classe C.

( ) deve ser organizada com uma ou várias células/seções na estrutura organizacional da Agência Central do SIEx. Nas agências Classe A, Especiais (exceto Aditâncias) e Classe B, a célula de OSINT pode ser organizada, não sendo o caso a organização de célula de OSINT nas AI Classe C.

( ) deve ser organizada com uma ou várias células na estrutura organizacional de todas as AI do SIEx.

( ) pode ser organizada com uma ou várias células na estrutura organizacional de todas as AI do SIEx.

( )pode ser organizada com uma ou várias células na estrutura organizacional de todas as AI do SIEx, exceto nas AI Classe C .

( ) deve ser organizada com uma ou várias células na estrutura organizacional de todas as AI do SIEx, exceto nas AI Classe C .

7) Em situações de EMPREGO (Guerra/Não Guerra), a OSINT deve ser organizada com, no mínimo, 1 (uma) célula de OSINT:

( ) a partir do escalão Unidade.
( ) a partir do escalão Brigada.
( ) a partir do escalão Divisão.
( ) a partir do escalão Corpo de Exército.

ORGANIZAÇÃO

Considerações para a pergunta 8:

✓Nas operações, seja em situação de guerra ou de não guerra, a Cia Anl Intlg do BIM possui a missão, entre outras, de desdobrar a Central de Inteligência, por intermédio do Pel Anl Intlg, e compor a Cel Intlg do Centro de Coordenação das Operações (CCOp) do escalão apoiado (item 3.4.1 do Manual do BIM – EB70-MC-10.302)..

✓No ciclo da Inteligência Militar, a Cent Intlg participa de todas as fases. Na fase de obtenção, a Cent Intlg participa, por meio da Célula de Análise (Cel Anl), na obtenção de dados, seja a partir de bancos de dados ou por meio de fontes abertas. Estes dados, juntamente com os demais dados levantados, são integrados na fase de produção, tendo como produtos os conhecimentos elaborados pela Cel Anl (item 3.4.2 do Manual do BIM – EB70-MC-10.302).

✓A Cent Intlg, em sua estrutura, deve contar com a participação de especialistas de todas as fontes de dados utilizadas na operação (Manual do BIM – EB70-MC-10.302). - De acordo com o fluxo de Inteligência durante as operações, têm-se que o "Ambiente de Análise" difunde PI/OB para o "Ambiente de Obtenção", composto pelo BIM, dentre outros meios (vide Fig 3-8 do Manual do BIM – EB70-MC-10.302).
✓A atual estrutura organizacional do BIM possui uma Companhia de Sensores de Fontes Tecnológicas (Cia Sns F Tecnl). A Cia Sns F Tecnl possui um Pelotão de Inteligência Cibernética, composto por 4 (quatro) grupos de Inteligência Cibernética. A Cia Sns F Tecnl não possui fração especializada em OSINT, sobrecarregando as frações de Intlg Cibernética com ações de coleta, em detrimento das ações de busca. (vide Fig 6-1 do Manual do BIM – EB70-MC-10.302).

Fluxo de Intlg durante as Operações

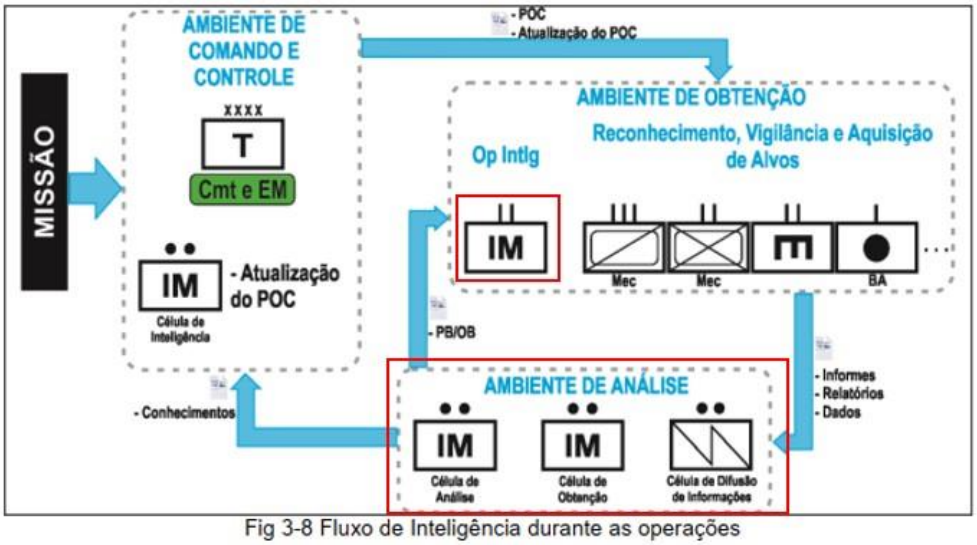


Fig 3-8 Fluxo de Inteligência durante as operações

Organização do BIM

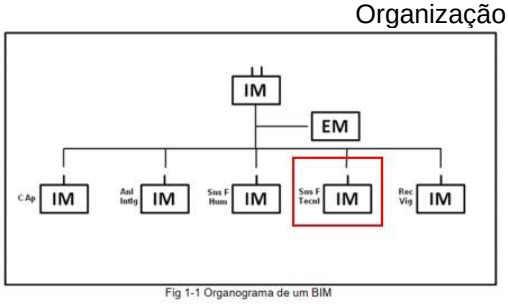


Fig 1-1 Organograma de um BIM

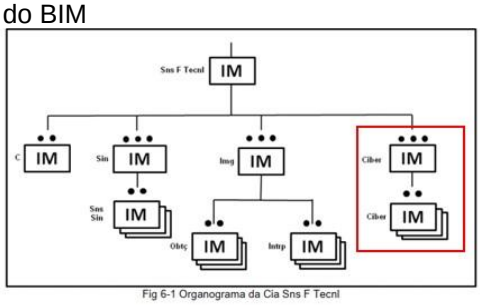


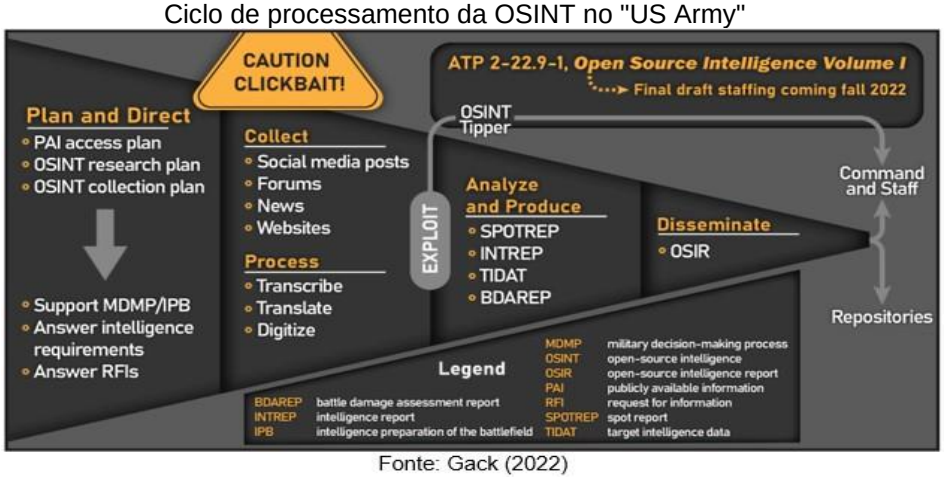
Fig 6-1 Organograma da Cia Sns F Tecnl

8) Coerente com essa doutrina, o QUÊ o Sr acredita que deve ocorrer com a atual estrutura organizacional dos BIM, para recepcionar a estruturação da OSINT no SIEx?
( ) deve ser reestruturada, com a inclusão de um Pelotão de OSINT na Cia Sns F
( ) deve ser reestruturada, alterando-se a estrutura do Pel Intlg Ciber da Cia Sns F Tecnl, com a inclusão de frações de OSINT nesse Pelotão.
( ) não deve ser reestruturada sob a ótica da da OSINT no SIEx, uma vez que a fração de Intlg Ciber do BIM tem condições de atender a todas as demandas de coleta de dados em fontes abertas e de busca de dados protegidos no ambiente cibernético.
( ) não deve ser reestruturada sob a ótica da da OSINT no SIEx, uma vez que a OSINT é uma atribuição de todos os integrantes da Célula de Análise de Inteligência da Central de Inteligência (item 3.4.8.10 do Manual do BIM – EB70-MC-10.302).

DOUTRINA
Considerações para a pergunta 9:
✓Atualmente, os países que possuem a OSINT estruturada em seus respectivos Sistemas de Inteligência possuem PRODUTOS doutrinários de OSINT (sem classificação), que são amplamente compartilhados por e-mail ou qualquer sistema não classificado, com foco na Segurança Nacional, garantindo que os usuários possam acessar o produto em um dispositivo móvel em qualquer lugar do mundo e a qualquer hora. Cita-se como exemplos de produtos de OSINT difundidos nessas condições:

- ESTADOS UNIDOS: Relatório de Inteligência de Fonte Aberta (OSIR – Open Source Intelligence Report);
- CANADÁ: Resumo Diário de OSINT (OSINT Daily Summaries); e
- AUSTRÁLIA: Relatório de OSINT (OSINT Report).

Ciclo de processamento da OSINT no "US Army"



Fonte: Gack (2022)

9) Sobre uma eventual proposta de inclusão de PRODUTOS de OSINT no SIEx, COMO o Sr acredita que esse processo deve funcionar?

( ) Informe, Informação, REI, Aprec ou SUMINT, com restrição de acesso, com difusão pelo sistema institucional de transmissão de documentos classificados do SIEx.

( ) Relatórios não classificados de OSINT, com difusão pelo sistema institucional de transmissão de documentos classificados do SIEx.

( ) Relatórios Temáticos/Resenhas Críticas de OSINT não classificados, com difusão por intermédio de e-mail ou aplicativos de mensageria institucionais/institucionalizados, no âmbito do SIEx, cabendo compartilhamento no âmbito do SISBIN, com texto de redação livre, permitidas variações em sua forma e conteúdo, de acordo com as necessidades do cliente.

MATERIAL e INFRAESTRUTURA

Considerações para a pergunta 10:

✓No processo de estruturação da OSINT no SIEx, a disponibilidade e a qualidade do MATERIAL (equipamentos, suprimentos e recursos) e da INFRAESTRUTURA (instalações e tecnologia) podem ter um impacto significativo no desempenho das funções do Analista de OSINT.

10) No processo de estruturação da OSINT no SIEx, sob a ótica do "MATERIAL" e da "INFRAESTRUTURA", o Sr acredita que

( ) é necessário amplo investimento em material, sobretudo MTIC, e amplo investimento em novas instalações com tecnologia para suportar o trabalho das frações de OSINT, uma vez que atualmente, o material e a infraestrutura do SIEx não suportam a implementação da OSINT.

( ) não é necessário investimento nem em material nem em novas instalações,
uma vez que atualmente, o material e a infraestrutura do SIEx possuem boas condições para recepcionar a estruturação da OSINT, serão necessários apenas ajustes internos nas agências.

***** FIM *****

OBRIGADO PELA SUA VALIOSA CONTRIBUIÇÃO.
ANTES DE TUDO, INTELIGÊNCIA!

APÊNDICE B – MODELO DE RESENHA CRÍTICA

RESENHA CRÍTICA – 17 ABR 24

NÍVEIS DE ALERTA: ⚠ ALTO ⚠ MÉDIO ⚠ BAIXO

⚠ SITUAÇÃO CLIMÁTICA DO BRASIL (ATUALIZAÇÃO)

A partir de 15 FEV, um ciclone subtropical deve provocar precipitações volumosas em partes da Região SUDESTE. Segundo o CEMADEN, há **"risco alto" para eventos geológicos na Região Metropolitana de SÃO PAULO/SP, VALE DO PARAÍBA, LITORAL NORTE e BAIXADA SANTISTA, bem como no SUL FLUMINENSE**. A Região NORTE deve continuar recebendo grandes quantidades de precipitações, estando no período mais chuvoso do ano (inverno amazônico), que concentra até 70% do volume anual. **As condições meteorológicas previstas têm potencial para promover eventos geológicos de grandes proporções, com incremento das ações de Defesa Civil. A manutenção de precipitações nas áreas indicadas oferece condições desfavoráveis à infraestrutura rodoviária, com impactos para a BR-174 e a BR-369.**

⚠ SITUAÇÃO NA TERRA INDÍGENA YANOMAMI (ATUALIZAÇÃO)

Após a temática YANOMAMI ser enredo do carnaval deste ano, diversas **mídias internacionais, como *LE FIGARO, EL PAÍS* e *EURONEWS*, repercutiram críticas à situação dos YANOMAMIS.** Segundo dados da Operação CATRIMANI, até o momento, foram entregues mais de 5 mil cestas de alimentos às comunidades na TIY. **É muito provável o incremento da temática YANOMAMI na Dimensão Informacional, com reflexos para os Órgãos que assistem aos indígenas naquela região.**

⚠ FUGA DE PRESOS DA PENITENCIÁRIA FEDERAL DE MOSSORÓ/RN (PFMOS)

Em 14 FEV, dois presos fugiram da PFMOS. Os fugitivos são oriundos do ACRE e faccionados ao COMANDO VERMELHO. Em SET 23, ambos haviam sido transferidos para o Sistema Penitenciário Federal (SPF), após uma rebelião no Presídio de Segurança Máxima ANTÔNIO AMARO (RIO BRANCO/AC), que resultou na morte de cinco detentos. Esta é a primeira fuga de presos custodiados no SPF. Até o momento, consta que a fuga ocorreu por conta de uma falha estrutural da penitenciária. **A fuga de presos denota uma vulnerabilidade da Unidade Prisional (UP), não se descartando o envolvimento de funcionários da PFMOS. É provável que a Força Penal Nacional seja mobilizada para atuar na UP.**

⚠ COLÔMBIA/CUBA – POLÍTICA DE PAZ TOTAL (ATUALIZAÇÃO)

Em 11 FEV, CUBA aceitou o convite do Governo da COLÔMBIA para intermediar as negociações de paz entre o grupo dissidente da antiga guerrilha das FARC, a "Segunda Marquetalia", e o Governo colombiano. **O Chanceler cubano, BRUNO RODRÍGUEZ**, afirmou que CUBA "ratifica sua firme posição a favor da paz na COLÔMBIA". **É provável que o diálogo de paz não reduza a violência no país, o que mantém a tendência da atuação de Grupos Armados Organizados Residuais (GAO-r) dissidentes na região de fronteria, impactando o Entorno Estratégico brasileiro.**

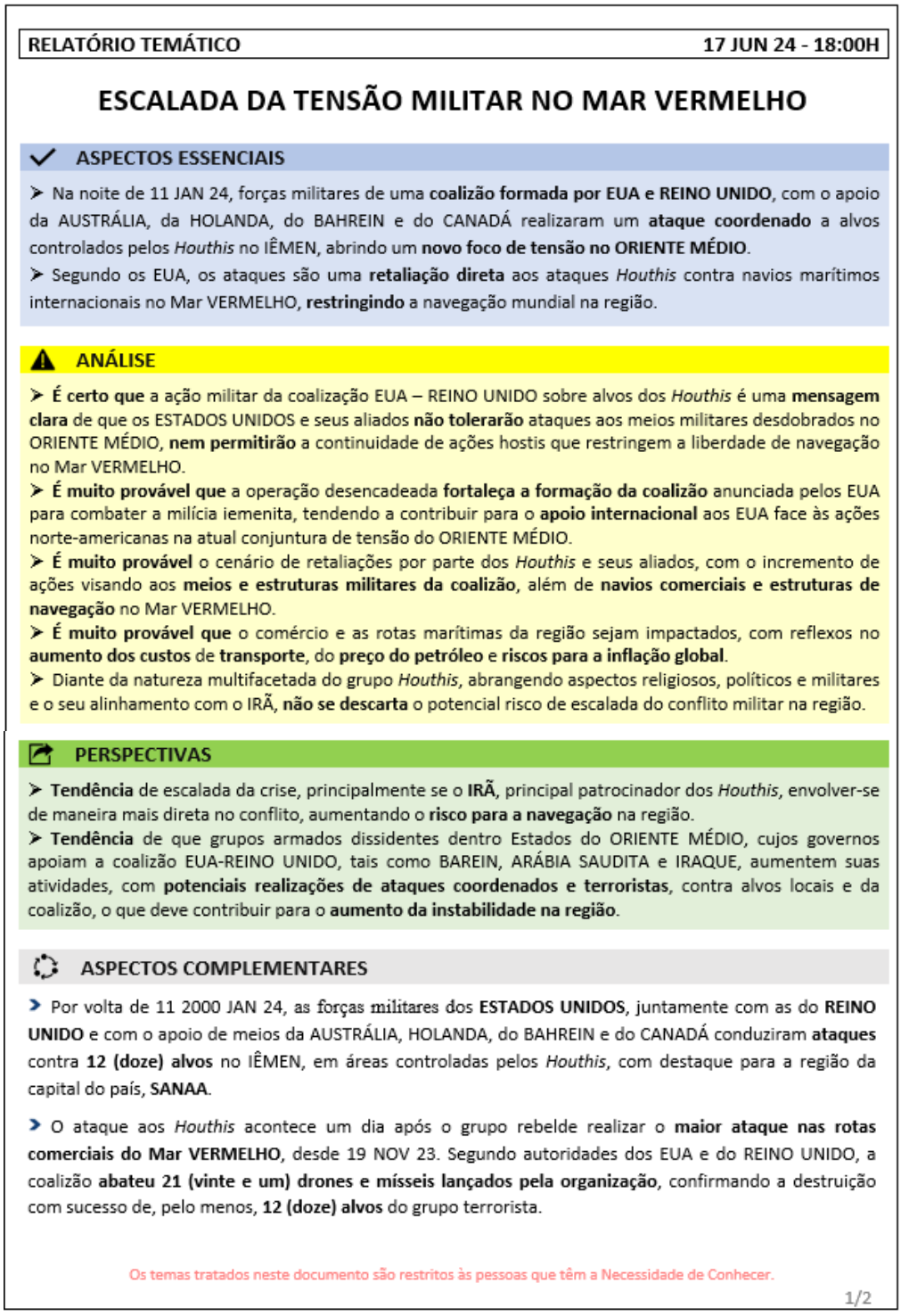
⚠ COLÔMBIA – CRISE NA SEGURANÇA PÚBLICA

Em 13 FEV, o Governo da COLÔMBIA decretou "Emergência Carcerária" em todos os centros de detenção do país, em resposta aos recentes homicídios, ataques e ameaças contra **os efetivos do Instituto Nacional Penitenciário e Carcerário (INPEC) colombiano.** O Decreto restringe visitas aos presos, limita as comunicações, transfere de presídios líderes de Organizações Criminosas (ORCRIM) e permite que a Força Pública efetue vigilância de penitenciárias. **É muito provável que as ORCRIM executem ações em resposta ao recrudescimento das operações de combate ao narcotráfico. A tendência é de escalada da crise de Segurança Pública no país, impactando o Entorno Estratégico brasileiro.**

◆◆◆FIM◆◆◆

Fonte: o autor.

APÊNDICE C – MODELO DE RELATÓRIO TEMÁTICO



RELATÓRIO TEMÁTICO **17 JUN 24 - 18:00H**

ESCALADA DA TENSÃO MILITAR NO MAR VERMELHO

ASPECTOS ESSENCIAIS

➢ Na noite de 11 JAN 24, forças militares de uma **coalizão formada por EUA e REINO UNIDO**, com o apoio da AUSTRÁLIA, da HOLANDA, do BAHREIN e do CANADÁ realizaram um **ataque coordenado** a alvos controlados pelos *Houthis* no IÊMEN, abrindo um **novo foco de tensão no ORIENTE MÉDIO**.

➢ Segundo os EUA, os ataques são uma **retaliação direta** aos ataques *Houthis* contra navios marítimos internacionais no Mar VERMELHO, **restringindo** a navegação mundial na região.

ANÁLISE

➢ **É certo que** a ação militar da coalização EUA – REINO UNIDO sobre alvos dos *Houthis* é uma **mensagem clara** de que os ESTADOS UNIDOS e seus aliados **não tolerarão** ataques aos meios militares desdobrados no ORIENTE MÉDIO, **nem permitirão** a continuidade de ações hostis que restringem a liberdade de navegação no Mar VERMELHO.

➢ **É muito provável que** a operação desencadeada **fortaleça a formação da coalizão** anunciada pelos EUA para combater a milícia iemenita, tendendo a contribuir para o **apoio internacional** aos EUA face às ações norte-americanas na atual conjuntura de tensão do ORIENTE MÉDIO.

➢ **É muito provável** o cenário de retaliações por parte dos *Houthis* e seus aliados, com o incremento de ações visando aos **meios e estruturas militares da coalizão**, além de **navios comerciais e estruturas de navegação** no Mar VERMELHO.

➢ **É muito provável que** o comércio e as rotas marítimas da região sejam impactados, com reflexos no **aumento dos custos** de **transporte**, do **preço do petróleo** e **riscos para a inflação global**.

➢ Diante da natureza multifacetada do grupo *Houthis*, abrangendo aspectos religiosos, políticos e militares e o seu alinhamento com o IRÃ, **não se descarta** o potencial risco de escalada do conflito militar na região.

PERSPECTIVAS

➢ **Tendência** de escalada da crise, principalmente se o **IRÃ**, principal patrocinador dos *Houthis*, envolver-se de maneira mais direta no conflito, aumentando o **risco para a navegação** na região.

➢ **Tendência** de que grupos armados dissidentes dentro Estados do ORIENTE MÉDIO, cujos governos apoiam a coalizão EUA-REINO UNIDO, tais como BAREIN, ARÁBIA SAUDITA e IRAQUE, aumentem suas atividades, com **potenciais realizações de ataques coordenados e terroristas**, contra alvos locais e da coalizão, o que deve contribuir para o **aumento da instabilidade na região**.

ASPECTOS COMPLEMENTARES

➢ Por volta de 11 2000 JAN 24, as forças militares dos **ESTADOS UNIDOS**, juntamente com as do **REINO UNIDO** e com o apoio de meios da AUSTRÁLIA, HOLANDA, do BAHREIN e do CANADÁ conduziram **ataques** contra **12 (doze) alvos** no IÊMEN, em áreas controladas pelos *Houthis*, com destaque para a região da capital do país, **SANAA**.

➢ O ataque aos *Houthis* acontece um dia após o grupo rebelde realizar o **maior ataque nas rotas comerciais do Mar VERMELHO**, desde 19 NOV 23. Segundo autoridades dos EUA e do REINO UNIDO, a coalizão **abateu 21 (vinte e um) drones e mísseis lançados pela organização**, confirmando a destruição com sucesso de, pelo menos, **12 (doze) alvos** do grupo terrorista.

Os temas tratados neste documento são restritos às pessoas que têm a Necessidade de Conhecer.

1/2

Fonte: o autor.

- Segundo declaração do Presidente dos EUA, os ataques são uma resposta direta aos ataques *Houthis* sem precedentes contra navios marítimos internacionais no Mar VERMELHO, com o incremento da utilização de mísseis balísticos antinavio, pela primeira vez na história.

- Autoridades dos EUA destacaram que o grupo já realizou mais de **27 (vinte e sete) ataques, desde NOV 23**, e acusam o IRÃ de financiar e fornecer armamento aos rebeldes, dissidentes do Governo oficial do IÊMEN, e planejar as operações contra navios comerciais no Mar VERMELHO.

Fig 1-2 Locais de ataques a navios no Mar VERMELHO

Fig 2-2 Áreas controladas pelo Houthis no IÊMEN

- Em 10 JAN 24, o Conselho de Segurança das Nações Unidas aprovou uma resolução exigindo que os *Houthis* acabassem com os ataques a navios mercantes e comerciais, medida que precedeu a resposta da coalizão EUA – REINO UNIDO contra a milícia.

- Recentemente, o grupo terrorista prometeu continuar os ataques até que ISRAEL interrompa o conflito em GAZA, e alertaram que atacariam navios de guerra dos EUA no Mar VERMELHO, caso o próprio grupo de fosse alvo.

- Nos últimos meses, os ataques *Houthis* perturbaram o comércio internacional na principal rota entre a EUROPA e a ÁSIA, que representa cerca de 15% do tráfego marítimo mundial, comprometendo o comércio e ameaçando a liberdade de navegação no Mar VERMELHO.

O ASSUNTO CONTINUA EM PROCESSAMENTO

♦♦♦FIM♦♦♦

Fonte: o autor.