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

**CURSO AVANÇADO DE INTELIGÊNCIA PARA OFICIAIS**

**TRABALHO DE CONCLUSÃO DE CURSO (TCC)**

# A OSINT NO LEVANTAMENTO DE AMEAÇAS CONTRA O EXÉRCITO BRASILEIRO

**Brasília**

**2023**

Maj ALLAN PAULO ALVARENGA SANTOS

# A OSINT NO LEVANTAMENTO DE AMEAÇAS CONTRA O EXÉRCITO BRASILEIRO

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

Orientador: Ten Cel CARLOS EDUARDO **TAVARES** DE LIMA

S237o Santos, Allan Paulo Alvarenga

A OSINT no levantamento de ameaças contra o Exército Brasileiro / Allan Paulo Alvarenga Santos – 2023.
36 f.

Orientador: Carlos Eduardo Tavares de Lima
Trabalho de Conclusão de Curso (Especialização em Análise de Inteligência) - Escola de Inteligência Militar do Exército (EsIMEx), Brasília – DF, 2023.

1. Inteligência 2. Fontes abertas 3. Open Source Intelligence 4. Ameaças
5. Produção de conhecimento I. Título.

Maj ALLAN PAULO ALVARENGA SANTOS

# A OSINT NO LEVANTAMENTO DE AMEÇAS CONTRA O EXÉRCITO BRASILEIRO

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 _____de_____de 2023.

COMISSÃO DE AVALIAÇÃO:

_____
CARLOS EDUARDO TAVARES DE LIMA – TC - Presidente
Escola de Inteligência Militar do Exército

_____
JOSÉ ALVES JÚNIOR – TC - Membro
Escola de Inteligência Militar do Exército

## RESUMO

A cada ano, o acesso a uma quantidade crescente de dados via internet se torna mais amplo e a quantidade de material compartilhado a cada minuto é surpreendente. Esse cenário traz consigo mudanças rápidas e constantes, o que dificulta a previsão de cenários e a identificação das principais ameaças, como costumava ser feito anteriormente. Nesse sentido, a utilização da Open Source Intelligence (OSINT) passa a desempenhar papel fundamental na produção de conhecimento de inteligência, permitindo ao Exército Brasileiro (EB) obter informações atualizadas, diversificadas e confiáveis. Entretanto, para isso, faz-se necessário o entendimento das capacidades dessa ferramenta para que possam ser da melhor forma aproveitadas, além de entender as suas limitações. Devido ao grande volume de informações existente na área de atuação da OSINT, cresce de importância a utilização de instrumentos de apoio a análise e o emprego criterioso dos métodos de análise. Entretanto, é destacado o protagonismo do analista de inteligência, personagem essencial para o sucesso das atividades provenientes de fontes abertas. Desta forma, este trabalho buscou analisar a importância da utilização das fontes abertas, observando as diferentes fases existentes na pesquisa em fontes abertas para melhor atender às necessidades do EB e garantir uma preparação eficaz para enfrentar os desafios atuais.



Palavras-chave: Inteligência. Fontes abertas. Open Source Intelligence. Ameaças. Produção de conhecimento.

## ABSTRACT

Every year, access to an increasing amount of data via the internet becomes broader, and the amount of material shared every minute is astounding. This scenario brings about rapid and constant changes, making it difficult to predict scenarios and identify major threats, as it used to be done before. In this sense, the use of Open Source Intelligence (OSINT) plays a fundamental role in intelligence knowledge production, enabling the Brazilian Army (EB) to obtain up-to-date, diverse, and reliable information. However, in order to achieve this, it is necessary to understand the capabilities of this tool so that they can be best utilized, as well as to understand its limitations. Due to the vast amount of information in the OSINT field, the use of analysis support tools and the judicious use of analysis methods become increasingly important. However, the role of the intelligence analyst is emphasized as crucial for the success of activities derived from open sources. Thus, this work sought to analyze the importance of using open sources, considering the different phases involved in open source research in order to better meet the needs of the EB and ensure effective preparation to face current challenges.



Keywords: Intelligence. Open sources. Open Source Intelligence. Threats. Knowledge production.

**SUMÁRIO**

ALLAN PAULO ALVARENGA SANTOS[1]

## 1 INTRODUÇÃO

Antes do advento dos satélites e de outros meios tecnológicos avançados, para a coleta de informações, os profissionais militares desenvolveram a inteligência de informações de código aberto para obter conhecimento e buscar a percepção do entendimento dos territórios, povos, ameaças potenciais e forças beligerantes. Porém, o mundo está se reinventando na internet, com quantidades de informações que se tornam imediatamente disponíveis ao público (*United States,* 2012).

Apoiada no constante desenvolvimento tecnológico, a internet nas últimas décadas passou a ser um recurso crucial, não apenas para a comunicação, mas também pelo acesso a quantidades surpreendente de dados.

A cada ano, a quantidade de dados acessíveis via internet cresce e a quantidade de material compartilhado a cada minuto é impressionante (STEELE, 2016).

Esse cenário permite um volume de mudanças com relativa agilidade, tornando muito difícil prever cenários e enxergar as principais ameaças como era feito antes. Atualmente, estar pronto para lidar com o inesperado é mais importante que investir tempo em planejamentos muito detalhados (PIRES, 2018).

A conectividade e a interdependência são fatores que ampliam a complexidade. Os modelos tradicionais de gestão de riscos e tomada de decisão não são suficientes para lidar com o número de variáveis desses contextos interconectados. Fica cada vez mais difícil prever os resultados de ações isoladas, pois elas são facilmente inseridas e dissipadas dentro desse ambiente (PIRES, 2018).

Essas características passaram a ser conceituadas com o acrônimo VUCA[2], para tentar exemplificar essas mudanças do mundo atual.

A concepção deste mundo contemporâneo, torna-se um terreno fértil para a

---

[1] Oficial de Comunicações do Exército Brasileiro - Academia Militar das Agulhas Negras. Pós-graduado em Operações Militares – Escola de Aperfeiçoamento de Oficiais. allan.paulo@eb.mil.br.

[2] VUCA é uma sigla em inglês, formada pela primeira letra das palavras: Volatility (volatilidade), Uncertainty (incerteza), Complexity (complexidade) e Ambiguity (ambiguidade). É um conceito relacionado aos imprevistos e rapidez com que as mudanças ocorrem em diversos cenários (PIRES, 2018).

prática de ações hostis, com a atuação de atores diversos, sem a definição clara de seus interesses.

Entretanto, esse mesmo ambiente, sendo adequadamente explorado, pode ser útil no levantamento das ameaças. Nas palavras de Paul Kolbe, Diretor do Intelligence Project, estão agora disponíveis “vastos tesouros de dados” que, “se analisados e propostos, pode fornecer informações impressionantes sobre áreas que antes só podiam ser descobertas por meio de métodos arriscados, caros e coleta restrita de inteligência” (MORROW, 2022).

Segundo Leite (2014), hoje existe uma diversidade de dados disponíveis capazes de auxiliar a atividade de inteligência. Essas informações podem oferecer material relevante quando bem processadas e analisadas. Neste ambiente concentram-se informações provenientes de variadas fontes. A OSINT (*Open Source Intelligence*) assume papel fundamental na coleta de dados. Através dela é possível obter documentos oficiais não restritos, acompanhar a dinâmica econômica, social e política de um país, monitorar as tendências da mídia e as produções técnico-científicas.

O manual canadense, CFJP 2-8 (Open-Source Intelligence), (CANADÁ, 2016), que aborda o assunto, confirma a OSINT como parte integrante da inteligência em todos os níveis de comando. Seu papel e suas contribuições evoluem à medida que as condições do ambiente operacional exigem. Se realizado rigorosamente e de forma deliberada, OSINT tem inúmeras vantagens e é capaz de fornecer informações necessárias, aprimorando a produção de conhecimento, principalmente para os níveis operacional e tático.

Pela complexidade e volume de dados que são trabalhados pela OSINT, fica evidenciado a importância da utilização de processos para a produção de conhecimento que podem ser bem visualizados na doutrina militar de inteligência.

No manual EB20-MF-10.107 (Inteligência Militar Terrestre) é citado o Ciclo de Inteligência, que é definido como uma sequência ordenada de atividades, segundo a qual dados são obtidos e conhecimentos são produzidos e colocados à disposição dos usuários de forma racional.

Ainda na mesma publicação, é acrescentado que este faseamento é cíclico, compreendendo a orientação, a obtenção, a produção, a difusão. Além disso, é destacado que a credibilidade dos conhecimentos produzidos depende diretamente da constante reavaliação dos procedimentos executados durante o Ciclo de Inteligência e para que o produto da Inteligência Militar seja efetivo, é necessário que haja uma constante realimentação no ciclo de modo que ele se mantenha atualizado e capaz de responder às necessidades do usuário.

Desta forma, este trabalho buscou analisar como a OSINT pode trabalhar na produção de conhecimento dentro da conjuntura atual, observando as diretrizes e instrumentos vigentes, verificando as melhores formas de se otimizar no levantamento de ameaças contra o Exército Brasileiro (EB).

Assim, este trabalho buscou obter mais conhecimentos a respeito do tema: Os Produtos da OSINT para a Função de Combate Inteligência. Pela não existência de manual próprio, foi priorizado a pesquisa em manuais militares de outros países.

Diante do exposto, e da necessidade da inteligência se posicionar perante as mudanças do mundo atual, dando respostas oportunas e pertinentes as ameaças, surge o problema que norteará a presente pesquisa: Como a Função de Combate Inteligência poderá levantar as ameaças contra o Exército Brasileiro?

De modo que o tema não ficasse muito amplo, o assunto foi delimitado da seguinte forma: A OSINT no levantamento de ameaças contra o Exército Brasileiro.

O presente trabalho tem como objetivo enfatizar a importância do uso das fontes abertas na produção de conhecimento para o Exército Brasileiro (EB), visando atender de maneira eficaz às necessidades de conhecimento sobre suas ameaças e garantir uma preparação adequada para enfrentá-las. Em um contexto em constante evolução, é crucial que o EB tenha acesso a informações atualizadas e diversificadas, e as fontes abertas desempenham um papel fundamental nesse processo.

De modo a conduzir o leitor a melhor compreensão do tema proposto, inicialmente abordaremos o emprego da Inteligência Militar na produção de conhecimento, abordando suas disciplinas, em seguida será relatado a definição de

ameaça, bem como seus principais atores. Por fim apresentaremos o emprego da OSINT na produção de conhecimento com seus respectivos produtos.

## 2 A INTELIGÊNCIA NA IDENTIFICAÇÃO DAS AMEAÇAS

A Inteligência Militar (IM), em qualquer nível de atuação, possui como denominador comum a permanente identificação das ameaças, minimizando incertezas e buscando oportunidades para o sucesso das operações (BRASIL, 2015b).

Ainda na mesma publicação, na definição de conceito, a IM é destacada a sua busca permanente pela redução do grau de incerteza existente nos diversos ambientes operacionais. Para isso, é fundamental a análise e integração dos dados obtidos pelos diversos sensores. A identificação das ameaças e oportunidades é o primeiro dos resultados que a IM deve fornecer aos comandantes.

No âmbito do Exército Brasileiro, até a publicação do manual EB-20-MF-10.107 (Inteligência Militar Terrestre), a atividade de Inteligência trabalhava apenas com as tradicionais fontes de Inteligência, quanto a natureza de sua origem: humanas, imagens, sinais e cibernética.

A partir da referida publicação, foi introduzida, também, as Disciplinas de Inteligência, que dizem respeito ao material, aos sistemas e aos procedimentos utilizados para observar, explorar, armazenar e difundir informação referente à situação, ameaças e outros fatores julgados úteis para uma operação (LEAL, 2019).

São divididas da seguinte forma: Inteligência de Fontes Humanas (HUMINT), Inteligência de Imagens (IMINT), Inteligência Geográfica (GEOINT), Inteligência por Assinatura de Alvos (MASINT), Inteligência de Fontes Abertas (OSINT), Inteligência de Sinais (SIGINT), Inteligência Cibernética (CYBINT), Inteligência Técnica (TECHINT) e Inteligência Sanitária (MEDINT). Tais classificações são de acordo com a natureza da fonte ou do órgão de obtenção que a explora.

Dentre as disciplinas citadas, a OSINT se destaca no exercício da Atividade de Inteligência Militar (AIM), citada por grande parte da Comunidade de Inteligência (CI) como “a fonte primária de coleta de dados” devido a sua natureza onipresente e sua capacidade de ser amplamente compartilhada (SILVA, 2022).

Consoante a este pensamento, o EB reconhece a OSINT como uma fonte básica de inteligência, afirmando que os seus produtos reduzem as demandas às outras disciplinas de inteligência, de modo a liberá-las para focarem na obtenção de dados que não possam ser adquiridos em fontes abertas (BRASIL, 2015b).

Para a concretização de suas atividades, a Inteligência está estruturada no Sistema de Inteligência do Exército (SIEx), que é formado por órgãos e pessoas do Exército Brasileiro (EB) que, sob a responsabilidade dos comandantes, chefes ou diretores, estão envolvidos na execução das atividades e tarefas de Inteligência ou que estão ligados à sua regulamentação e normatização.

Sua responsabilidade é de produzir, continuamente, os conhecimentos necessários para que o EB permaneça preparado e em condições de ser empregado contra quaisquer ameaças à soberania ou à integridade do país, atuando em Operações no Amplo Espectro em atendimento às situações de emprego previstas na Constituição e na Estratégia Militar de Defesa (BRASIL, 2015b).

Cabe destacar que na conjuntura atual, em relação ao grande volume de dados disponíveis, vários especialistas afirmam que a grande maioria dos dados levantados são originários da pesquisa em fontes abertas, sugerindo que o papel da OSINT é realmente significativo.

Corroborando com essas opiniões, o General de Divisão americano, Samuel V. Wilson, ex-Diretor da Agência de Inteligência de Defesa (Defense Intelligence Agency), comentou que a OSINT tem capacidade de fornecer cerca de 90% das informações utilizadas pela comunidade de inteligência (RASAK, 2021).

Assim, o emprego da OSINT tem relevante participação na AIM, contribuindo na necessidade de produção de conhecimento sobre ameaças, sobretudo nas circunstâncias do cenário atual.

## 2.1 DEFINIÇÃO DE AMEAÇA

Pela definição do manual EB20-MC-10.207 (Inteligência), ameaça é qualquer conjunção de atores, entidades ou forças com intenção e capacidade de realizar

ação hostil contra o país e seus interesses nacionais, com possibilidades de por intermédio da exploração de deficiências, causar danos ou comprometer a sociedade nacional (a população e seus valores materiais e culturais) e seu patrimônio (território, instalações, áreas sob jurisdição nacional e o conjunto das informações de seu interesse). Também pode ocorrer sob a forma de eventos não intencionais (naturais ou provocados pelo ser humano).

Ainda em relação a ameaça, no manual EB20-MF-10.107 (Inteligência Militar Terrestre) e definida da seguinte forma:

> Uma ameaça pode ser concreta (identificável) ou potencial. Pode ser definida como a conjunção de atores, estatais ou não, entidades ou forças com intenção e capacidade de realizar ação hostil contra o país e seus interesses nacionais, com possibilidades de causar danos à sociedade e ao patrimônio. Ameaças ao país e a seus interesses nacionais também podem ocorrer na forma de eventos não intencionais, por causas naturais. (BRASIL, 2ª Ed, 2015b, parte II – Termos e Definições).

No manual EB70-MC-10.220 (Contrainteligência), a definição de ameaça é desmembrada facilitando seu entendimento, descrevendo todas as partes pertences ao conceito e é relacionada ao EB.

Sistematicamente, a ameaça ocorre quando existe a combinação de ator, motivação e capacidade de realizar ação hostil, por intermédio da exploração de deficiências, comprometer as informações, afetar o material, o pessoal e seus valores, bem como as áreas e instalações, podendo causar danos ao Exército (BRASIL, 2019a).

Por este conceito, ator sob o ponto de vista das ameaças, é dividido em integrantes do público interno ou externo. A constituição do Público Interno é formada por militares da ativa e inativos, ex-combatentes e servidores civis, todos do Exército, bem como, naquilo que couber seus dependentes e os alunos dos Colégios Militares. Para o Público Externo o conceito é direcionado para pessoas, grupos de pessoas ou organizações não incluídos no público interno (BRASIL, 2019a).

Já a motivação, acontece quando o ator ao ter a intenção de atingir objetivos, realiza ações para alcançá-los. Para isso, precisa de estímulos que podem estar relacionados a questões financeiras, ressentimentos, vaidades, vingança, estresse, insatisfação, dentre outras.

Para a concretização da ameaça, o ator motivado precisa ter a capacidade de executar sua ação desejada. No manual EB70-MC-10.220, é salientado que quanto mais alternativas e liberdade de ação o ator dispuser, maior será a sua capacidade de agir.

Para identificar sua capacidade de agir, é considerado se o autor tem ao seu dispor, recursos e qual a “habilitação técnica para a realização de tarefas, bem como sua liberdade de ação para empregar esses recursos, explorando as deficiências identificadas por ele” (BRASIL, 2019a, p.2-4).

Ao entender a definição de ameaça, fica destacado a importância de identificar e examinar os diversos atores como parte fundamental da produção de conhecimento. Além disso, o entendimento do que provoca as motivações e o que permite sua a capacidade de agir, serão informações relevantes na tarefa da Inteligência no levantamento das ameaças contra o EB, aproveitando-se das características de OSINT.

## 2.2 AS AMEAÇAS DO MUNDO CONTEMPORÂNEO

A Política Nacional de Inteligência (PNI), documento de mais alto nível de orientação da atividade de Inteligência no País, define os parâmetros e limites de atuação da atividade de Inteligência e de seus executores e estabelece seus pressupostos, objetivos, instrumentos e diretrizes, no âmbito do Sistema Brasileiro de Inteligência (BRASIL, 2016).

Em seu texto, foi considerado como principais ameaças aquelas que apresentam potencial capacidade de pôr em perigo a integridade da sociedade e do Estado e a segurança nacional do Brasil.

Para balizar as atividades dos órgãos pertencentes ao Sistema Brasileiro de Inteligência, as ameaças foram priorizadas da seguinte forma: Espionagem, Sabotagem, Interferência Externa, Ações contrárias à Soberania Nacional, Ataques cibernéticos, Terrorismo, Atividades ilegais envolvendo bens de uso dual e tecnologias sensíveis, Armas de Destruição em Massa, Criminalidade Organizada, Corrupção e Ações Contrárias ao Estado Democrático de Direito (BRASIL, 2016).

Nas análises e projeções apresentadas pelo Cenário de Defesa 2020-2039, publicado pelo Ministério da Defesa, as principais ameaças foram atribuídas aquelas com implicações para a Segurança e a Defesa. Foram citadas: a dependência tecnológica, a escassez mundial de recursos naturais, manipulação da opinião pública, terrorismo, crime organizado transnacional, tensões sociais no Brasil, hostilidades contra cidadãos e bens brasileiros no exterior, insuficiente capacidade operacional das Forças Armadas, insegurança de sistemas de informação, catástrofes naturais e pandemias, fricções e tensões na América do Sul e militarização do Atlântico Sul (BRASIL, 2017).

O manual EB20-MF-10.102 (Doutrina Militar Terrestre), ao descrever sobre o caráter difuso das ameaças, define ameaça de maneira similar aos manuais de Inteligência Militar abordados anteriormente.

Ainda em relação ao manual, comenta-se que:

> as ameaças ao País e aos seus interesses nacionais também podem ocorrer na forma de eventos não intencionais, naturais ou provocados pelo homem. Apesar da ocorrência de conflitos bélicos, com o empenho de numerosos efetivos, a declaração formal de guerra entre Estados deixou de ser a regra (BRASIL, 2ª Ed, 2019b, p. 2-5).

Destaca-se ainda, a preocupação em identificar o adversário, sendo regular ou não, devido ao ambiente de incertezas. Acrescenta-se ainda, o relevante crescimento de grupos transnacionais e/ou insurgentes, tendo apoio ou não, de grupos ou países, que ampliou a disseminação de novas ameaças que devem ser enfrentadas com o emprego de forças de defesa (BRASIL, 2019b).

Buscando quais seriam as ameaças para o EB, também foi considerado a diretriz do Comandante do Exército 2023-2026. Em suas palavras, disse que: “Minha intenção é acelerar as ações de transformação e de modernização do Exército Brasileiro que proporcionem capacidades para enfrentar as ameaças mais relevantes ao País e contribuam para o desenvolvimento nacional.”

Dando continuidade as suas diretrizes, o Comandante do EB, em suas premissas, citou preocupação com as ameaças presentes e futuras do cenário contemporâneo, principalmente aquelas que possam pôr em risco a segurança, o patrimônio, a soberania e a integridade territorial brasileira.

Além disso, citou a necessidade de exercitar a Inteligência Militar Terrestre em todos os escalões da Força, contribuindo para a identificação de ameaças e oportunidades que orientarão o processo decisório do Comandante.

Diante do contexto atual, as ameaças configuram-se de maneira diferente. Ocorre uma migração de um cenário convencional com características bem definidas, para um emergente com aspectos distintas e difusos (quadro 1).

**Quadro 1 – Cenários**

| AMEAÇA CONVENCIONAL | AMEAÇA EMERGENTE |
|---|---|
| **CARACTERÍSTICAS** | |
| **governamental** | não governamental |
| **convencional** | não convencional |
| **ordens de batalha conhecidas** | trabalho dinâmico ou aleatório |
| **desenvolvimento linear** | desenvolvimento não linear |
| **regra de engajamento** | sem restrições |
| **doutrina conhecida** | doutrina desconhecida ou inexistente |
| **ativos de inteligência conhecidos** | não domínio dos meios de inteligência empregados |

Fonte: STEELE (2018) adaptado pelo autor.

Essas mudanças passam a exigir maior capacidade dos órgãos de inteligência e para isso é necessário o desenvolvimento de habilidades em condições de se depararem com essas novas ameaças. Cabe destacar ainda, a relevância da produção de conhecimento, que precisa se adaptar as novas exigências, entregando produtos com agilidade e oportunidade.

# 3 O EMPREGO DA OSINT NA PRODUÇÃO DE CONHECIMENTO

As novas tecnologias são revolucionárias. Seu impacto atenderia aos critérios de Thomas Kuhn para revoluções científicas[3]. Através do ciberespaço e sua alta capacidade formativa, as novas tecnologias permitem que as pessoas encontrem, criem e disponibilizem publicamente uma quantidade massiva de informações (BENES, 2013).

Importante considerar, que a igualdade de acesso e a possibilidade de criação nas fontes abertas, ajuda as autoridades a combater as ameaças que possam impactar ao Estado, é neste aspecto que a OSINT se posiciona como considerável ferramenta na produção de conhecimento dos perigos existentes.

Entretanto, com o amplo volume de dados disponíveis, é fundamental estabelecer formas para separar as informações pertinentes, identificar as corretas, processá-las e utilizá-las de forma eficiente na produção de conhecimento.

Deste modo, a forma de conduzir o estudo dos dados cresce de relevância, porque a atividade de análise fica pressionada devido aos efeitos provocados pela quantidade de dados, qualidade diversa e a importância dos fatos que exige urgência em seu processamento.

Nesse sentido, Benes (2013) cita que neste ambiente o analista deve ser capaz de reunir, julgar e classificar informações; conhecer e lidar com limitações; e entender os diferentes atores (pessoas, organizações e instituições), para conseguir uma melhor combinação de informações.

## 3.1 AS FONTES ABERTAS

O manual americano ATP 2-22.9 (Open-Source Intelligence), define fonte aberta como sendo todas as informações que qualquer pessoa ou grupo, tornaram públicos, sem a expectativa de privacidade, não se limitando a pessoas físicas.

[3] A Estrutura das Revoluções Científicas é um livro sobre a história da ciência publicado no ano de 1962 pelo filósofo Thomas Kuhn. Ele argumentou que períodos de continuidade de uma ciência são interrompidos por períodos revolucionários, cujas anomalias geram novos paradigmas que questionam os anteriores, levando a pesquisa científica a novos caminhos (CHIBENI, 2020).

Complementando, são as 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 (BRASIL, 2015b).

Pela diversidade de origens, carece o entendimento dos elementos que a compõem. A seguir, para ilustrar, é apresentado uma divisão por tipos de fontes, utilizada pelo Exército Americano.

**Quadro 2 – Divisão das Fontes EUA**

| *Media* | *Components* | *Elements* |
|---|---|---|
| **Public Speaking** | Speaker | • Sponsor • Message • Relationship |
| | Format | • Conference • Lecture • Debate • Rally • Demonstration • Loud speakers • Speeches • Talk shows |
| | Audience | • Location • Composition |
| **Public Documents** | Graphic | • Drawing • Photograph • Engraving • Print • Painting • Posters • Graffiti |
| | Recorded | • Compact data storage device • Hard disk • Tape • Digital video disk |
| | Printed | • Book • Periodical • Brochure • Pamphlet • Newspapers • Report • Magazines • Novelties • Government releases • Non-government releases • "Dumpster diving" • Leaflets • Annuals • Business cards |
| **Public Broadcasts** | Radio | • Low frequency AM radio • VHF FM radio • Medium frequency AM radio • Satellite radio • Short wave radio • Standard wave radio |
| | Television | • Ku band satellite television • VHF and UHF terrestrial television • Advertisements • Motion pictures |
| **Internet Web Sites** | Communications | • Chat • Web cam • E-mail • Web cast • News; newsgroup • Web log |
| | Databases | • Commerce • Government • Education • Military organizations |
| | Information (Web page content) | • Commerce • Government • Education • Military organizations |
| | Services | • Dictionary • Geospatial • Directory • Search and URL lookup • Downloads • Technical support • Financial • Translation |
| AM amplitude modulation<br>FM frequency modulation<br>UHF ultrahigh frequency | | URL uniform resource locator<br>VHF very high frequency |

Fonte: ATP 2-22.9 (Open Source Intelligence).

Ao analisar essa distribuição de fontes primária, é possível inferir que o emprego da OSINT pode ser priorizado para os sites de internet. Isso é possível devido a facilidade de ferramentas disponíveis e tecnologia, que permitem que

documentos impressos e transmissões públicas, como o rádio e a TV, estejam também disponíveis na internet.

Isso é possível porque as mídias tradicionais estão migrando para a Internet, buscando maior interação a um custo relativamente baixo.

Cabe destacar que uma parcela significativa da internet não é acessível por meio de uma simples pesquisa. Muito informações residem na Deep Web. As informações na Deep Web não são indexadas por simples ferramentas de busca, portanto, não aparece como resultado de uma consulta de pesquisa básica. A Deep Web inclui informações de código aberto, no entanto, técnicas especiais devem ser usadas para coletar.

## 3.2 A OSINT NO LEVANTAMENTO DE INFORMAÇÕES

A internet fez com que os dados derivados de uma fonte aberta fossem mais práticos e úteis, tornando-se, por outro lado, mais difícil de gerir. Ademais, a quantidade de informações disponíveis e a diversidade de formatos desses dados criam obstáculos na produção do conhecimento.

É preciso saber identificar o que é relevante, filtrar e processar todas as informações e extrair um conhecimento. No entanto, mesmo com software sofisticado, pode acontecer do analista da OSINT, devido ao volume do fluxo de dados, perder uma informação importante (LEITE, 2014).

Desta forma, a aplicação de métodos adequados, configura-se como alicerces para o desenvolvimento do conhecimento das fontes de OSINT.

Segundo o manual EB20-MC-10.207 (Inteligência), os trabalhos da Inteligência são desenvolvidos seguindo as fases do ciclo de inteligência (ciclo de produção do conhecimento). Esse ciclo compreende uma sequência de atividades mediante a qual a inteligência obtém e reúne dados, transforma-os em conhecimento de Inteligência.

Analisando a doutrina americana, o ciclo de inteligência é semelhante, entretanto, é destacado, que pelas particularidades da disciplina de inteligência

OSINT, as fases do ciclo de inteligência deverão se comportar de maneira mais dinâmicas.

Inicialmente é realizado o planejamento, identificando os requisitos da informação que se quer buscar, identificar os alvos e determinar as técnicas de coleta mais apropriadas.

O manual United States (2018), salienta a importância da realização da avaliação de risco para conduzir as atividades durante a definição da técnica de coleta adequada para a fonte de interesse. No manual americano, é destacado que tais procedimentos, são para manter o anonimato, e para que dessa forma, o alvo não interfira nas ações de coleta, bloqueando, alterando, manipulando as fontes.

O próximo passo é a montagem do plano de coleta. Devendo ser consideradas as seguintes características: identificação de fontes abertas; descrição de como acessar essas fontes; formato para compilar os dados; metodologia de coleta; e divulgação do plano. Com o plano preparado, inicia-se o processo de coleta.

Após a coleta, o analista de OSINT precisa avaliar as informações obtidas. No manual ATP 2-22.9 (Open-Source Inteligente), são citados alguns indicadores que podem ser utilizados nessa avaliação, como: volume, variedade e disponibilidade. Isso é importante para avaliar a confiabilidade dos dados obtidos, distinguindo as informações objetivas e factuais das tendenciosas e enganosas. A classificação da informação é baseada no julgamento subjetivo do avaliador e a precisão das informações anteriores produzidas pela mesma fonte.

Na mesma direção, o manual CFJP 2-8 (Open-Source Intelligence), da Força Conjunta Canadense, apresenta princípios básicos que orientam a coleta e a produção de conhecimento utilizando a OSINT. São os seguintes:

a) foco. As atividades OSINT devem ser conduzidas para atingir o objetivo proposto;

b) compatível. As atividades da OSINT devem ser conduzidas em conformidade com todas as leis, políticas, diretivas e ordens;

c) eficiente. As atividades de coleta OSINT devem garantir que a coleta desnecessária seja reduzida ou eliminados, quando apropriado;

d) confiável. Existe o risco de informações de código aberto serem tendenciosas ou conter desinformação. A veracidade e validade de qualquer informação devem ser observadas pelo analista;

e) acessível. Os especialistas em OSINT devem ter acesso à mais ampla variedade de materiais possível, incluindo fontes pagas e gratuitas;

f) compartilhado. A informação só é útil se for acessível. Material de código aberto coletado devem ser compartilhados o mais amplamente possível;

g) flexível. O OSINT deve estar condições de responder às mudanças, influenciada por novas situações e novas informações; e

h) seguro. As operações OSINT devem ser conduzidas de tal maneira que não comprometam os procedimentos de segurança ou o acesso contínuo das fontes.

Para ilustrar essa importante etapa na obtenção de dados, a seguir são listadas algumas ferramentas que podem ser utilizadas na coleta de dados (DE CASTRO, 2022):

a) buscadores. São websites especializados em busca de dados e informações contidas na internet a partir de uma palavra escrita pelo usuário. Os principais buscadores são: Google, Yahoo, Bing, Duckduckgo, Asklcom, Aol, Baidu (chinês) e Yandex;

b) metabuscadores. Os metabuscadores têm o mesmo objetivo dos buscadores, porém funcionam aproveitando os índices criados pelos próprios buscadores para obter e proporcionar ao usuário os melhores resultados. As ferramentas mais conhecidas são: Carrot, Dogpile, Startpage e Metacrawler;

c) outras Plataformas a título de exemplificação:

**- IHS Jane’s Defense & Security Intelligence & Analysis**

A Jane’s é uma empresa que atua no campo da Defesa. Ela possui um vasto banco de dados, atuando em diversos países ao redor do mundo. Ela pertence ao grupo IHS, que também é outra empresa que com atuação em diferentes áreas. Além do campo da Defesa, divulga informações sobre energia, economia, risco geográfico, sustentabilidade e abastecimento. É possível acessar suas publicações através de aquisições de seus serviços.

**- Military Periscope**

Assim como a IHS Jane's Defence, oferece uma gama de dados relativos à Defesa mundial. Fundada em 1986 nos EUA, é considerada uma das melhores ferramentas de OSINT para obtenção de informações nessa área. Ela dispões de uma cobertura detalhada sobre as Forças Armadas, Organizações Terroristas, Equipamentos, Armas, Missões de Paz, Ordens de Batalha, Planos e Programas Militares, entre outros dados de centenas de países do mundo. Suas informações são constantemente atualizadas.

**- Stratfor Global Intelligence**

Atua em análises geopolíticas, oferecendo produtos atualizados em diversos segmentos de interesse no cenário mundial. Alguns campos de sua atuação são: político, econômico, cibernético, energético, conflito Rússia-Ucrânia, ciência e tecnologia, entre outros. Fundada em 1996 nos Estados Unidos, seu acesso é possível por meio de assinatura.

**- Intelligence On line**

Com atuação direta na área de Inteligência, trabalha na elaboração de notícias sobre os principais Serviços de Inteligência no mundo e possui colaboradores e correspondentes espalhados em todos os continentes mundiais.

Como apresentado neste capítulo, a OSINT tem grande capacidade na produção de conhecimento para o levantamento de ameaças. Como vantagens, destacam-se os seguintes tópicos:

a) As fontes abertas permitem atualização constante através do acompanhamento em tempo real das modificações das ameaças, facilitando a adaptação de estratégias e a tomada de decisão;

b) diversidade de informações possibilita a ampliação de conhecimento em diferentes contextos, como políticos, econômicos, militares, sociais e culturais. Permitindo uma compreensão ampla do ambiente operacional;

c) a verificação cruzada de dados permite comparar e contrastar diferentes informações, verificando sua confiabilidade e validade. Isso contribui para evitar a propagação de informações falsas ou imprecisas;

d) Ao contrário de outras fontes de informação, que muitas vezes exigem altos investimentos em equipamentos, as fontes abertas são geralmente acessíveis gratuitamente ou a custos relativamente baixos;

e) permite que o analista de inteligência corrobore e adicione novas informações a outras coletas que possam estar em curso; e

f) OSINT geralmente também pode ser compartilhada com um público mais amplo, incluindo outros órgãos de inteligência.

Por outro lado, importante salientar as desvantagens, que devem ser consideradas em todas as fases do emprego da OSINT para produzir conhecimento. O manual canadense CFJP 2-8 (Open-Source Intelligence) as representa da seguinte forma:

a) informações de código aberto podem conter imprecisões, perspetivas tendenciosas, informações irrelevantes informação e desinformação. Verificar a confiabilidade e a credibilidade da fonte ajuda a mitigar esse problema; no entanto, a verificação da fonte não elimina estas questões;

b) exposição não intencional de informações a adversários e potenciais inimigos podem facilmente resultar da não observância dos procedimentos segurança. Dada a prevalência do uso da Internet, é fundamental uma abordagem focada e disciplinada por todos que trabalham com OSINT;

c) as buscas OSINT podem resultar em um grande volume de informações, cujo processamento pode ser muito trabalhoso e demorado. A utilização de ferramentas que possibilitem o gerenciamento e processamento dos dados coletados podem reduzir significativamente o número de pessoal envolvido e dar maior agilidade;

d) as tecnologias de informação e Internet em rápida evolução podem modificar rapidamente os processos e tecnologias de OSINT empregados. Isso pode ser mitigado com uma gestão adequada de fontes pagas e gratuitas e o uso efetivo de coleta; e

e) as ações de OSINT exigem o uso de pessoal especializado, que devem acompanhar o avanço tecnológico com formação contínua.

Consoante o que foi apresentado nesse capítulo, fica evidenciado que a OSINT tem uma importante capacidade de explorar várias fontes gerando um grande volume de dados. Entretanto, para transformar essas informações em conhecimento, fica evidenciado a importância de empregar uma exploração sistemática, simbolizada pelo Ciclo de Inteligência.

## 4 PRODUTOS DA OSINT

Os produtos de Inteligência devem ser oportunos, relevantes e detalhados, concebidos de forma a possibilitar a consciência situacional e a tomada de decisão com segurança. A precisão e o detalhamento desses produtos têm influência direta no sucesso da operação. Entretanto, sua validade é limitada no tempo (BRASIL, 2015a).

Consoante ao descrito anteriormente, o manual EB70-MT-10.401 (Produção do Conhecimento de Inteligência), diz que o produto da atividade de Inteligência é materializado, essencialmente, pelo conhecimento[4] de Inteligência, cujo propósito básico é subsidiar a tomada de decisão, em todos os níveis. Esses conhecimentos apresentam as seguintes características:

a) resultam da aplicação de uma metodologia própria, na coleta e/ou busca de dados, e na produção;

b) buscam reduzir o grau de incerteza existente nos diversos ambientes operacionais, estabelecendo suas implicações (consequências) e reflexos para o Exército Brasileiro; e

c) vários usuários podem utilizar os conhecimentos produzidos.

Para atender a essas características, a OSINT necessita essencialmente do analista. Para uma efetiva produção de conhecimento, ele deve ser um especialista, com profundo conhecimento do problema que está sendo abordado. Coletores e analistas devem ser capazes de reduzir os déficits analíticos causados por tentativas de desinformação ou pela má qualidade do dado. Além disso, uma notícia de jornal, por exemplo, pode ser interpretada de diversas formas por um analista da CIA, da Agência Brasileira de Inteligência (ABIN) ou do *Mossad*, dependendo de suas prioridades, de seus interesses e de seus parâmetros (LEITE, 2022).

---

[4] É o produto do Ciclo de Inteligência Militar, como resultado do processamento de dados, informações ou conhecimentos anteriores, utilizando-se de metodologia específica, visando à avaliação ou ao estabelecimento de conclusões sobre fatos ou situações (BRASIL, 2015b).

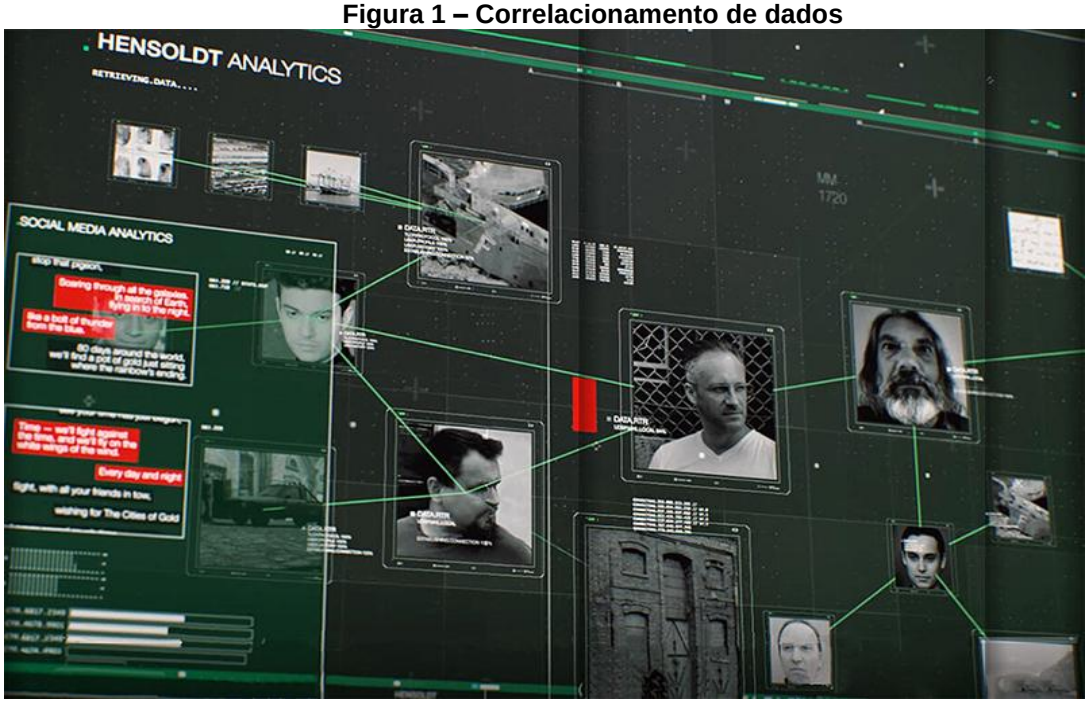
Outra abordagem interessante sobre Fontes Abertas é que seus produtos reduzem as demandas às outras disciplinas de Inteligência, de maneira que essas se dediquem somente a obter dados que não possam ser adquiridos pelas fontes abertas (BRASIL, 2015b).

Seus produtos são extremamente eficazes reforçando a inteligência derivada de outras disciplinas, como HUMINT (Inteligência Humana), SIGINT (Inteligência de Sinais), IMINT (Inteligência de Imagens) e GEOINT (Inteligência Geográfica).

A seguir, serão apresentados alguns produtos de OSINT, que podem contribuir no levantamento de ameaças.

Identificação de atores e grupos, é um deles. A OSINT permite a identificação e o monitoramento de atores e grupos que possam representar ameaças à segurança do EB ou do país. Isso inclui organizações criminosas, grupos terroristas, entre outros. Para isso são levantados o perfil digital, que consiste na coleta de informações disponíveis publicamente sobre indivíduos ou grupos, como seus perfis em redes sociais, sites pessoais, artigos publicados, comentários em fóruns, entre outros.

**Figura 1 – Correlacionamento de dados**



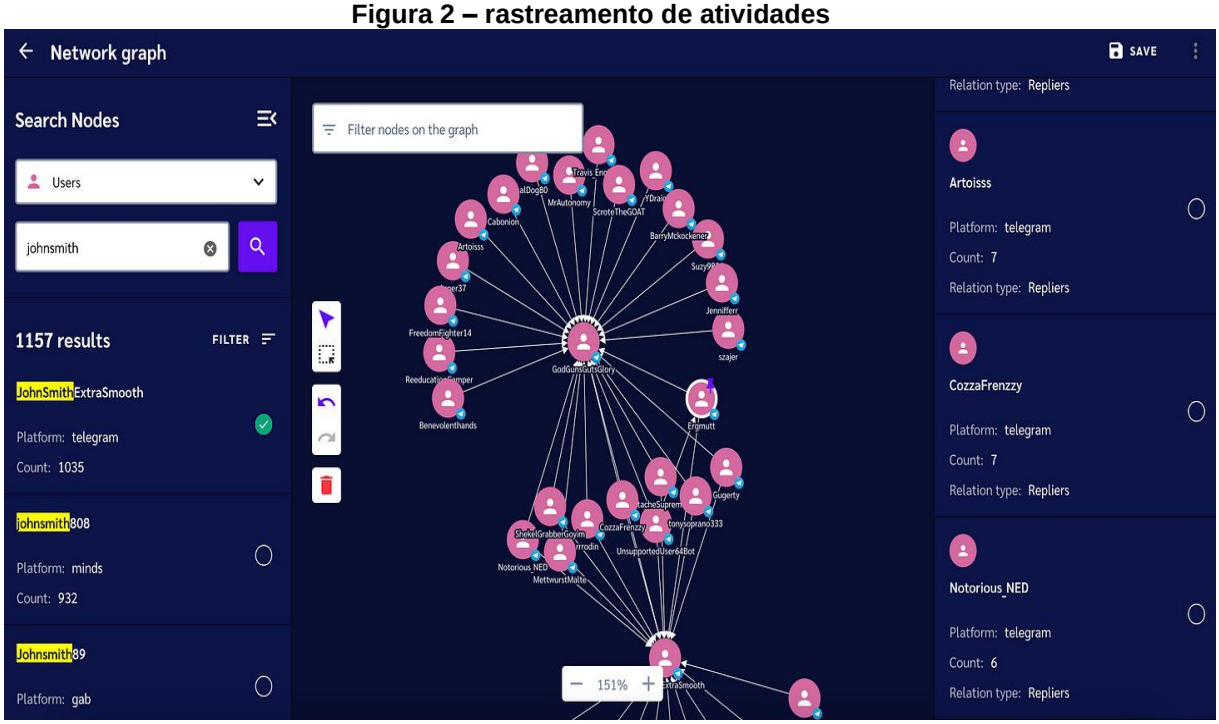

Fonte: PADILHA (2022).

Para tal finalidade, a análise de redes sociais é de extrema importância por auxiliar na identificação de conexões e relacionamentos entre atores e grupo, permitindo a revelação de hierarquias, estruturas organizacionais, influências e até mesmo ligações com outros atores ou entidades relevantes.

Outro produto é o monitoramento de redes sociais. Através da OSINT, é possível monitorar as atividades e comunicações em redes sociais, fóruns online e outras plataformas digitais, buscando identificar possíveis ameaças e acompanhar as tendências e discussões relevantes.

Uma forma de se levantar as informações é através do rastreamento de atividades, onde é monitorado as ações online, como postagens em blogs, fóruns, redes sociais e plataformas de compartilhamento de conteúdo. Essa vigilância pode ajudar a identificar padrões de comportamento, preferências, objetivos e até mesmo possíveis intenções ou ameaças.

**Figura 2 – rastreamento de atividades**

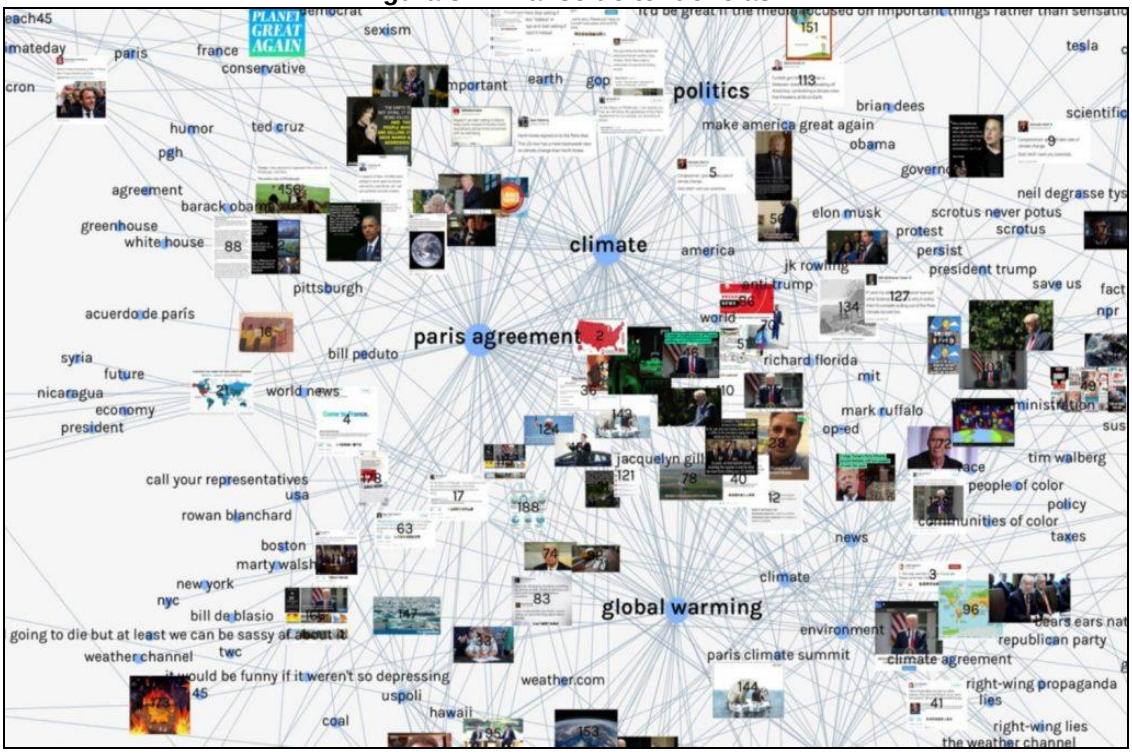



Fonte: CREPES (2023).

Destaca-se também a análise de tendências e padrões que é realizada com o acompanhamento de conversas e discussões em tempo real nas mídias sociais. Isso permite identificar tópicos emergentes, padrões de comportamento, opiniões

públicas e tendências populares. Além disso, pode ser feito a análise de notícias veiculados na mídia, que ajudam na identificação de tendências, eventos relevantes e mudanças no cenário político, social, econômico ou tecnológico.

**Figura 3 – Análise de tendências**




Fonte: MEIRELLES (2021).

Outra forma interessante é na observação de especialistas, influenciadores e líderes de opinião em diversos campos. Essas personalidades frequentemente compartilham opiniões, previsões e análises em suas áreas de atuação, o que pode ajudar a identificar tendências emergentes e padrões relevantes.

A avaliação de riscos também pode ser considerado um produto de OSINT, fornecendo informações atualizadas e relevantes para apoiar a tomada de decisão e na implementação de medidas de segurança apropriadas. Uma das formas de conseguir é no monitoramento de notícias, reportagens e postagens em mídias sociais relacionadas a eventos atuais, crises, desastres naturais, instabilidade política, ameaças de segurança e outros acontecimentos relevantes.

Além disso, deve-se acompanhar fontes governamentais e regulatórias, verificando informações divulgadas por esses órgãos relacionadas a riscos. Isso

pode incluir alertas de segurança, relatórios de agências de inteligência, diretrizes de saúde e segurança, entre outros. O acesso a essas fontes de informação ajuda na identificação e compreensão dos riscos impostos por regulamentos e políticas governamentais.

Ademais, a partir das informações coletadas, a OSINT também pode auxiliar na identificação de possíveis vulnerabilidades nas estruturas, instalações e sistemas do EB. Isso possibilita a adoção de medidas preventivas e o fortalecimento das defesas. Isso é possível na coleta de informações sobre sistemas operacionais, software, hardware e tecnologias utilizadas em uma organização ou em uma infraestrutura específica.

Essas informações podem incluir versões, atualizações, configurações, vulnerabilidades conhecidas e possíveis falhas de segurança. O acompanhamento de fóruns, grupos e comunidades online voltados para a segurança da informação ajudam nesses conhecimentos por serem espaços frequentemente utilizados por especialistas em segurança. O monitoramento dessas fontes pode fornecer percepções valiosas sobre novas vulnerabilidades ou ameaças emergentes.

Ainda demonstrando a diversidade de produtos, a OSINT tem capacidade em entregar produtos para resposta a desastres. Os desastres naturais têm uma dinâmica caótica própria, com cada incidente sendo totalmente único. Como resultado, é difícil formular protocolos de resposta que sejam eficazes de forma confiável em todos os setores.

Os primeiros sinais e relatos de desastres naturais aparecem e evoluem rápida e prontamente on-line, o que significa que a mídia social costuma ser um recurso mais atualizado do que os sistemas internos de detecção das autoridades. As ferramentas de OSINT podem monitorar eventos em tempo real mantendo as autoridades informadas e gerando geolocalizações específicas.

Outra importante entrega com o emprego das ferramentas da OSINT é na identificação e mitigação de ações de Operações Psicológicas[5]. As tecnologias de

[5] são campanhas de informação destinadas a influenciar a opinião, o raciocínio e as emoções para controlar as ações de indivíduos, grupos e até governos. Notícias falsas e desinformação podem ser muito perturbadoras e afetam significativamente pessoas e instituições (BRASIL, 2018).

OSINT oferecem maneiras eficientes de neutralizar a disseminação de desinformação. Usando algoritmos adequados, essas ferramentas podem varrer uma vultosa quantidade de dados e sinalizar uma infinidade de informações falsas e suas respectivas fontes.

Além desses produtos citados, a OSINT através de suas capacidades, passou a atuar em certos campos de coleta de dados de forma exclusiva. Cita-se como exemplo o levantamento de indicadores de localização; exploração de metadados embutidos em arquivos digitais, incluindo imagens e vídeos; exploração de dados de transação financeira, incluindo criptomoedas e transferências em moeda estrangeira; detecção de bots[6], usando volume de transmissão e padrões de transmissão online; e exploração de conteúdo da dark web.

Perante o exposto, evidencia-se que as entregas produzidas pela OSINT possuem amplitude na busca de ameaças, trabalhando com grande quantidade de informações, que corroboram no levantamento de ameaças contra o EB.

[6] abreviatura de robô – é um programa de software que executa tarefas automatizadas, repetitivas e pré-definidas. Os bots normalmente imitam ou substituem o comportamento do usuário humano (KLUSAITÈ, 2023).

## 5 CONCLUSÃO

O principal propósito deste trabalho foi destacar a relevância do uso de fontes abertas na geração de conhecimento, visando atender de maneira mais eficaz às demandas do EB no que se refere à compreensão de suas ameaças e à preparação adequada para enfrentá-las.

Com base no contínuo avanço tecnológico, a internet tem se tornado um recurso vital nas últimas décadas, desempenhando um papel crucial não apenas na comunicação, mas também no acesso a uma quantidade imensa de informações.

Esse cenário destaca a necessidade de profissionais de inteligência com habilidades adaptativas, flexíveis e inovadoras para enfrentar os desafios desse mundo em constante mudança.

As considerações iniciais buscaram caracterizar a importância da OSINT na atividade de inteligência, principalmente em um cenário incerto com mudanças constantes, exigindo profissionais cada vez mais ágeis e adaptáveis.

No decorrer da pesquisa, verificou que a quantidade crescente de dados produzidos e armazenados, juntamente com a variedade de fontes disponíveis, cria um cenário propício para o uso da OSINT para a produção de conhecimento. Ao analisar dados de mídias sociais, notícias e outras fontes abertas, é possível obter informações relevantes sobre intenções, planos e atividades de atores maliciosos.

Entretanto, devido ao grande volume de informações, foi verificado que alguns aspectos deveriam ser relacionados para a construção do embasamento lógico e teórico, fundamentado através do ciclo de inteligência, para que permitisse mostrar a capacidade de produção de conhecimento da OSINT, respeitando suas capacidades e limitações.

No prosseguimento da linha de raciocínio, foi observado que a OSINT consegue ter uma abordagem ágil e adaptativa, permitindo atualizações constantes oferecendo respostas mais eficazes às ameaças emergentes e em constante evolução.

As pesquisas realizadas indicaram como principais vantagens a menor intrusão comparada com outras formas de inteligência, permitindo coletar informações sem a necessidade de intervenções diretas. Além disso, é uma opção

mais acessível em termos de custo, tornando-se uma opção viável mesmo com recursos limitados. No tocante as desvantagens, destacam-se a qualidade e a confiabilidade das informações obtidas, e a sobrecarga de informações.

No entanto, é importante ressaltar que a OSINT não deve ser vista como uma solução isolada, mas como uma parte integrante de um processo de inteligência mais amplo. Ela complementa outras disciplinas de inteligência, fornecendo informações valiosas que podem ser usadas para aprimorar e validar a inteligência obtida por meio de outras fontes.

Em última análise, este trabalho destaca alguns desafios que devem ser mitigados. Ressalta-se o gerenciamento de grandes volumes de dados, onde será pertinente o desenvolvimento de capacidades para coletar, analisar e filtrar grandes quantidades de informações provenientes das fontes abertas, garantindo a eficiência na produção de conhecimento. Além disso, é essencial verificar a confiabilidade e autenticidade dos dados, evitando possíveis informações enganosas ou manipuladas.

Destaca-se ainda a importância do treinamento e capacitação, para uma utilização mais efetivas com as fontes abertas, desenvolvendo habilidades de pesquisa e análise.

Sendo assim, as ideias aqui apresentadas corroboraram no entendimento que os produtos da OSINT têm capacidade para desempenhar um papel fundamental no levantamento de ameaças, oferecendo uma abordagem valiosa para a inteligência.

Em suma, a OSINT desempenha um papel fundamental no levantamento de ameaças, fornecendo uma perspectiva abrangente e acessível por meio de informações de fontes abertas. Sua capacidade de coletar dados relevantes, identificar padrões e tendências, e se adaptar rapidamente às mudanças no cenário de ameaças a torna uma ferramenta indispensável para as atividades de inteligência no cenário atual.

## REFERÊNCIAS


AFONSO, Leonardo Singer. Fontes abertas e Inteligência de Estado. **Revista Brasileira de Inteligência**. Brasília: Abin, v. 2, n. 2, p. 49-62, abril de 2006.

BENES, Libor. OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm. **Journal of Strategic Security**. Number 5, volume 6, fall 2013.

BLOCK, Ludo; PETROVSKI, Andrej. **Open Source Intelligence Navigator for Investigative Journalists**. 2021. Disponível em: https://bird.tools/wp-content/uploads/2022/03/OSINT.pdf. Acesso em: 15 de maio de 2023.

BRASIL. **DECRETO Nº 8.793, DE 29 DE JUNHO DE 2016**. Fixa a Política Nacional de Inteligência. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm#:~:text=DECRETO%20N%C2%BA%208.793%2C%20DE%2029,que%20lhe%20confere%20o%20art. Acesso em: 27 fev. 2023.

BRASIL. Exército Brasileiro. **Conceito Operacional do Exército Brasileiro Operações de Convergência 2040 (EB20-MF-07.101)**. 1ª Edição, 2023. Portaria – EME/CEx nº 971, de 10 de fevereiro de 2023, publicada no Boletim do Exército nº7, de 17 de fevereiro de 2023.

BRASIL. Exército Brasileiro. **Manual de Campanha – Contrainteligência (EB70-MC-10.220)**. 1ª Edição, 2019a. Portaria nº 076-COTER, de 09 de julho de 2019, publicada no Boletim do Exército nº 30, de 26 de julho de 2019.

BRASIL. Exército Brasileiro. **Manual de Fundamento - Doutrina Militar Terrestre (EB20-MF-10.102).** 2ª Edição, 2019b. Portaria nº 326 - EME, de 31 de outubro de 2019, publicada no Boletim do Exército nº 45, de 08 de novembro de 2019.

BRASIL. Exército Brasileiro. **Manual de Fundamento - Inteligência (EB20-MC-10.207**). 1ª Edição, 2015a. Portaria nº 032 - EME, de 23 de fevereiro de 2015, publicada no Boletim do Exército nº 9, de 27 de fevereiro de 2015.

BRASIL. Exército Brasileiro. **Manual de Fundamento - Inteligência Militar Terrestre (EB20-MF-10.107).** 2ª Edição, 2015b. Portaria nº 031 - EME, de 23 de fevereiro de 2015, publicada no Boletim do Exército nº 9, de 27 de fevereiro de 2015.

BRASIL. Exército Brasileiro. **Manual Técnico – Produção do Conhecimento de Inteligência (EB70-MT-10.401)**. 1ª Edição, 2019. Portaria no 020-COTER, de 07 de março de 2019, publicada no Boletim do Exército nº 12, de 22 de março de 2019.

BRASIL. Exército Brasileiro. **Glossário de Termos e Expressões para uso no Exército (EB20-MF-03.109)**. 5ª Edição, 2018. Portaria nº 42 - EME, 20 de março de 2018.

BRASIL. Ministério da Defesa. **MANUAL DE ABREVIATURAS, SIGLAS, SÍMBOLOS E CONVENÇÕES CARTOGRÁFICAS DAS FORÇAS ARMADAS (MD33-M-02)**, 4ª ed., 2021. Portaria GM/MD nº 4034, de 01 de outubro de 2021, publicado no D.O.U, em 04 de outubro de 2021.

BRASIL. Ministério da Defesa. **Cenário de Defesa 2020 – 2039**. Assessoria Especial de Planejamento. 2017.

CANADA, Canadian Forces Joint**. Open-Source Intelligence** (**CFJP 2-8).** 2016.

CHIBENI, Silvio Seno. **Síntese de A Estrutura das Revoluções Científicas, de Thomas Kuhn**. 2020. Disponível em: https://www.unicamp.br/~chibeni/textosdidaticos/structure-sintese.htm. Acesso em: 25 maio 2023.

COMANDO DO EXÉRCITO. **Diretriz do Comandante do Exército 2023-2026**. Brasília, DF, fevereiro de 2023.

CREPS, Jake. **Tools, tactics, and techniques for network analysis using OSINT.** 2023. Disponível em: https://osintnewsletter.com/p/14. Acesso em: 06 de jun. 2023.

DE CASTRO, Leonardo Barbosa Ramos. **A Inteligência de fontes abertas durante a etapa de estudo das considerações civis na 2ª fase do PITCIC.** Brasília, 2022. Trabalho de Conclusão de Curso – Escola de Inteligência Militar do Exército.

GACK, Jarrod R. **The Open-Source Intelligence Conundrum: Creating the Discipline or Integrating the Data?** 2022. Disponível em: https://mipb.army.mil/articles/fy-2022/gack-osint-conundrum#lg=1&slide=0. Acesso em: 04 mar. 2023.

GARDNER, Dan; TETLOCK, Philip. **Superprevisões:** A arte e a ciência de antecipar o futuro. Tradução: Cassio de Arantes Leite, 1ª edição, Objetiva**,** 2016.

JÚNIOR, Paulo Eustáquio dos Santos. **O Sistema de Inteligência do Exército no contexto das novas ameaças**. Rio de Janeiro, 2018. Trabalho de Conclusão de Curso - Escola de Comando e Estado-Maior do Exército.

KLUSAITÈ, Laura. **O que são bots, tipos de bots e os perigos que eles trazem**. 2023. Disponível em: https://nordvpn.com/pt-br/blog/bot-o-que-e/. Acesso em: 25 de maio de 2023.

LEAL, Luís Henrique. CYBINT X OSINT: Semelhanças, diferenças e responsabilidades. **A Lucerna**, Brasília, ano VIII, p. 37 -41, julho de 2019.

LEITE, Sara Souza. O Emprego das Fontes abertas no Âmbito da Atividade de Inteligência Policial. **Revista Brasileira de Ciências Policiais**, Brasília, v. 5, n. 1, p. 11-45, janeiro/julho de 2014.

MEIRELLES, Pedro. **Introdução à análise de redes sociais online: quais são os principais conceitos?** 2021. Acesso em: https://insightee.com.br/blog/introducao-a-analise-de-redes-sociais-online-quais-sao-os-principais-conceitos/. Acesso em: 06 jun. 2023.

MORROW, Maria Robson. **Open Source Intelligence for National Security: The Art of the Possible.** 2022. Disponível em: https://www.belfercenter.org/publication/open-source-intelligence-national-security-art-possible. Acesso em: 15 abr. 2023.

PADILHA, Luiz. **Open Source Intelligence (OSINT) – Ferramenta de inteligência e combate ao terrorismo.** 2022. Disponível em: https://www.defesaaereanaval.com.br/ciencia-e-tecnologia/open-source-intelligence-osint-ferramenta-de-inteligencia-e-combate-ao-terrorismo. Acesso em: 06 jun. 2023.

PERRY, Chondra. Mídias Sociais e o Exército. **Military Review**, p. 50-55, maio-junho de 2010.

PIRES, Camila. **Mundo Vuca:** O que é e como se preparar. 2018. Disponível em:https://redeindigo.com.br/mundo-vuca-preparar/. Acesso em: 15 abr. 2023.

RASAK, Michael J. Event Barraging and the Death of Tactical Level Open-Source Intelligence. **Military Review**, p. 48 -57, January-February 2021.

SANTOS, Maíra Garcia. **A Migração das mídias tradicionais para aiInternet.** Brasília, 2007. Trabalho de Conclusão de Curso - Faculdade de Ciências Sociais Aplicadas.

SILVA, Iberê Mendes da Silva. **A integração de GEOINT e OSINT pelas agências de inteligência independentes.** Brasília, 2022. Trabalho de Conclusão de Curso – Escola de Inteligência Militar do Exército.

STEELE, Robert. **OSINT Done Right.** 2016**.** Disponível em: https://phibetaiota.net/2016/02/2016-robert-steele-on-osint-why-and-how/. Acesso em: 15 abr. 2023.

**The Wide-Ranging uses of OSINT in Military Intelligence**. 2022. Disponível em: https://blog.sociallinks.io/uses-of-osint-in-military-intelligence/. Acesso em: 15 abr. 2023.

UNITED STATES. **Open Source Intelligence Reader**. 2002. Disponível em: https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf. Acesso em: 28 fev. 2023.

UNITED STATES. Department of the Army. **Open-source intelligence (ATP 2-22.9)**. 1ª Edição. Washington, DC, 2012. Disponível em:< https://irp.fas.org/doddir/army/atp2-22-9.pdf>. Acesso em: 28 de fevereiro de 2023.

UNITED STATES. Department of the Army. **Open-source intelligence (ATP 2-22.9)**. 1ª Edição. Washington, DC, 2017.

UNITED STATES. Department of the Army. **Intelligence (FM 2-0)**. Washington, DC. 2010. Disponível em:< https://irp.fas.org/doddir/army/fm2-0.pdf>. Acesso em: 28 de fevereiro de 2023.

UNITED STATES. Department of the Army. **Intelligence (ADP 2-0)**. Washington, DC. 2018.

ZIÓŁKOWSKA, Agata. **Open Source Intelligence (OSINT) as an Element Of Military Recon**. 2018. Disponível em: https://securityanddefence.pl/pdf-103337-6164?filename=Open%20source%20intelligence.pdf. Acesso em: 15 abr. 2023.