Técnicas de Investigação e Perícia Computacional Baseadas em OSINT e HUMINT em Ações de Inteligência Cibernética

Renan Ferreira Meira[1], **João Benedito dos Santos Junior**[2]

[1]Aluno de Graduação do Curso de Ciência da Computação da PUC Minas *Campus* de Poços de Caldas – MG, Brasil
[2]Orientador e Docente do Departamento de Ciência da Computação da PUC Minas *Campus* de Poços de Caldas – MG, Brasil

renanferreirameira@hotmail.com, joao@pucpcaldas.br

Abstract. *This paper examines the use of OSINT tools and techniques jointed to HUMINT concept applied to cyber-intelligence actions. The research explores the integration of these approaches to enhance the collection, analysis, and interpretation of information in cyber intelligence activities. Case studies and comparative analyses are presented, highlighting the effectiveness and limitations of these methodologies. The results demonstrate that the combination of OSINT and HUMINT can provide valuable results for investigating cyber crimes, specially in terms of the contributions to the Law Enforcements.*

Resumo. *Este artigo aborda o uso de ferramentas e técnicas OSINT (Open Source Intelligence) e conceitos HUMINT (Human Intelligence) aplicados às ações de inteligência cibernética. A pesquisa explora a integração dessas abordagens para melhorar a coleta, análise e interpretação de informações em atividades de inteligência cibernética. São apresentados estudos de caso e análises comparativas, destacando a eficácia e as limitações dessas metodologias. Os resultados demonstram que a combinação de OSINT e HUMINT pode fornecer resultados valiosos para a investigação de crimes cibernéticos, especialmente no que se refere a contribuições para as Forças de Segurança e Lei.*

1 INTRODUÇÃO

A crescente dependência da sociedade moderna em relação às tecnologias da informação e comunicação tem impulsionado o surgimento de ameaças cibernéticas cada vez mais sofisticadas e abrangentes. Nesse contexto, a inteligência cibernética desempenha um papel crucial na detecção, prevenção e resposta a essas ameaças. No entanto, lidar com o ambiente complexo e em constante evolução do ciberespaço requer abordagens inovadoras e integradas.

O presente artigo tem como objetivo explorar o uso de ferramentas e técnicas OSINT (*Open-Source Intelligence*) em um conceito de HUMINT (*Human Intelligence*) aplicado às ações de inteligência cibernética relacionadas diretamente as atividades de investigação e perícia. A OSINT envolve a coleta e análise de informações disponíveis publicamente, enquanto a HUMINT se concentra na obtenção de informações por meio de interações humanas. A combinação dessas abordagens pode fornecer um panorama abrangente e detalhado do cenário cibernético, permitindo uma compreensão mais aprofundada das ameaças e oportunidades presentes [1][2].

Este artigo visa explorar as possibilidades de integração dessas metodologias para aprimorar as capacidades de coleta, análise e interpretação de informações em atividades de inteligência cibernética voltadas as respostas pós acontecimento. Serão apresentados estudos de caso e análises comparativas, destacando a eficácia e as limitações dessas

abordagens combinadas.

Espera-se que os resultados deste estudo contribuam para o avanço da área de inteligência cibernética, fornecendo *insights* para a investigação e perícia digital forense, visando tomada de decisões mais informadas e eficazes, e fortalecimento das capacidades de resposta em ambientes digitais. Ademais, este artigo também busca estimular a discussão e reflexão sobre o papel da inteligência humana e a importância da colaboração entre humanos e tecnologias na defesa contra ameaças cibernéticas.

No próximo capítulo, será apresentada uma revisão bibliográfica que busca abranger os principais conceitos, abordagens e técnicas relacionadas à OSINT, HUMINT e inteligência cibernética, proporcionando uma base teórica para a compreensão do tema em questão.

2 INTELIGÊNCIA CIBERNÉTICA

A inteligência cibernética refere-se à aplicação de metodologias de inteligência no contexto do ciberespaço. Ela envolve a coleta, análise e interpretação de informações relacionadas à segurança cibernética, visando obter *insights* sobre atividades maliciosas. A inteligência cibernética desempenha um papel fundamental na detecção, prevenção e resposta a ameaças cibernéticas [2].

No entanto, a inteligência cibernética enfrenta desafios significativos, como a necessidade de lidar com grandes volumes de dados e identificar informações relevantes de forma rápida e precisa. Além disso, a evolução constante das técnicas e táticas dos criminosos cibernéticos demanda atualizações contínuas nos métodos e ferramentas utilizados na investigação.

Neste capítulo, será realizada uma revisão da literatura sobre a inteligência cibernética, abordando conceitos, objetivos e principais desafios enfrentados nessa área.

2.1 VISÃO GERAL DA INTELIGÊNCIA CIBERNÉTICA

Os objetivos da inteligência cibernética são variados e abrangem desde a identificação precoce de ameaças e ataques cibernéticos até a avaliação de riscos, planejamento estratégico e apoio à tomada de decisões. Os principais propósitos da inteligência cibernética são: o fortalecimento das capacidades defensivas e o fornecimento de informações para investigações forenses digitais.

Fortalecer as capacidades defensivas das organizações contra ameaças digitais envolve a identificação e análise de ameaças emergentes, o monitoramento contínuo de sistemas e redes para detectar atividades suspeitas e a implementação de medidas de segurança proativas. Ao fortalecer suas defesas cibernéticas com base nas informações obtidas pela inteligência cibernética, as organizações podem mitigar riscos e minimizar o impacto de possíveis ataques, ponto que é inerente a inteligência cibernética mas que este artigo não buscará explorar.

Por outro lado, a inteligência cibernética também desempenha um papel crucial no fornecimento de informações para investigações forenses digitais. Quando ocorre um incidente, a análise forense é essencial para entender o que aconteceu, identificar os responsáveis e coletar evidências para processos legais. A inteligência cibernética pode fornecer dados valiosos sobre as táticas e técnicas utilizadas pelos invasores, rastrear suas atividades e até mesmo ajudar na atribuição de autoria. Essas informações são fundamentais para investigações bem-sucedidas e para a aplicação da justiça no mundo digital, sendo o principal foco deste artigo. [2][3].

2.2 DESAFIOS DA INTELIGÊNCIA CIBERNÉTICA

A inteligência cibernética enfrenta uma série de desafios que dificultam a obtenção e o uso efetivo de informações no ciberespaço. Um dos principais desafios enfrentados pela inteligência cibernética é lidar com a enorme quantidade de dados disponíveis. Com a rápida expansão das tecnologias digitais, a quantidade de informações relacionadas à segurança cibernética está em constante crescimento. Coletar, processar e analisar essa grande quantidade de dados representa um desafio significativo. É necessário adotar soluções eficientes de coleta e armazenamento de dados, além de utilizar técnicas avançadas de análise de dados para extrair informações relevantes.

A velocidade das ameaças cibernéticas é outro desafio crítico para a inteligência cibernética. Os adversários cibernéticos estão constantemente evoluindo e desenvolvendo novas táticas. As ameaças podem surgir e se propagar rapidamente, deixando pouco tempo para detecção e resposta, desta forma, a inteligência cibernética precisa ser ágil e adaptável, capaz de acompanhar o ritmo acelerado das ameaças cibernéticas. Isso requer uma combinação de tecnologias avançadas, processos eficientes e profissionais especializados que possam detectar e reagir rapidamente a ameaças emergentes.

Outro ponto também é que nem todas as fontes de informação são confiáveis e nem todos os dados disponíveis são precisos. A identificação de fontes confiáveis e a validação da qualidade das informações coletadas são aspectos críticos da inteligência cibernética, a falta de confiabilidade pode levar a decisões errôneas e ações ineficazes. É necessário estabelecer processos robustos de verificação e validação das fontes de informação, além de investir em parcerias e colaborações com organizações confiáveis e especialistas em segurança cibernética para garantir a qualidade e a integridade das informações utilizadas [2][3].

3 OPEN SOURCE INTELLIGENCE E HUMAN INTELLIGENCE

A *Open-Source Intelligence* (OSINT) é uma abordagem de coleta de informações que se baseia em fontes de dados abertas e disponíveis publicamente, como sites públicos, redes sociais, fóruns, blogs e bancos de dados online. Ela envolve a obtenção e análise de informações a partir dessas fontes para fins de inteligência cibernética. A OSINT tem se tornado cada vez mais relevante devido ao crescente volume de informações disponíveis online e à sua importância na compreensão de ameaças cibernéticas.

Por outro lado, a *Human Intelligence* (HUMINT) é uma disciplina tradicional da inteligência que envolve a obtenção de informações por meio de contato direto com fontes humanas. Ao contrário da OSINT, a HUMINT se concentra na interação humana como uma fonte primária de informações. Ela requer habilidades de relacionamento humano, empatia, persuasão e interpretação de comportamentos e intenções.

Tanto a OSINT quanto a HUMINT desempenham papéis importantes na coleta de informações para a inteligência cibernética. Enquanto a OSINT se concentra na análise de informações disponíveis publicamente, a HUMINT complementa esse processo ao fornecer informações exclusivas obtidas por meio de interações humanas [1][4][5].

A metodologia da OSINT envolve várias etapas para a coleta e análise de informações, a saber:

1. Planejamento: definir os objetivos da coleta de informações, identificar as fontes relevantes e estabelecer um plano de ação;
2. Coleta de dados: acessar fontes de dados abertas, como sites públicos, redes sociais, fóruns e bancos de dados online, para extrair informações pertinentes;
3. Triagem e seleção: avaliar a qualidade e a relevância das informações coletadas,

descartando dados irrelevantes ou de baixa confiabilidade;
4. Análise: examinar os dados coletados, identificar padrões e relações, e transformar as informações brutas em conhecimento acionável;
5. Validação: verificar a precisão e a confiabilidade das informações obtidas, buscando corroborar os dados com fontes adicionais sempre que possível.

Já quando se refere as metodologias voltadas à integração de OSINT e HUMINT, as seguintes etapas OSINT foram adicionadas:

1. Motores de busca: utilizar motores de busca convencionais, como o *Google* (*Dork* e *Regex*), para realizar pesquisas avançadas e explorar a internet em busca de informações relevantes;
2. Monitoramento de mídia social: acompanhar e coletar informações de plataformas de mídia social, como *Twitter*, *Facebook*, *LinkedIn* e *Instagram*;
3. *Scrapers* da *web*: utilizar ferramentas de *scraping* para extrair dados de sites e fóruns, automatizando o processo de coleta de informações;
4. Ferramentas de análise de dados: aplicar ferramentas de análise de dados, para visualizar e explorar os dados coletados, identificando padrões relevantes.

As principais ferramentas utilizadas estão disponíveis em *hubs* de inteligência cibernética tais como *Osint Framework* e *Osint – start.me*. São plataformas online que reúnem uma variedade de ferramentas e recursos de inteligência para investigações cibernéticas.

O *Osint Framework* é uma plataforma gratuita e aberta que fornece uma coleção organizada de recursos e ferramentas de OSINT. Ele abrange várias categorias, como pessoas, empresas, redes sociais, mecanismos de busca, governos, entre outros. Cada categoria inclui uma lista de recursos relevantes, como sites, ferramentas de pesquisa, APIs e plugins, que podem ser explorados para obter informações específicas.

O *Osint - start.me* é outro *hub* de inteligência cibernética que oferece uma compilação de ferramentas e recursos úteis para os profissionais de OSINT. Este por vez utiliza das possibilidades da plataforma start.me que fornece uma interface personalizável, onde você pode adicionar, organizar e acessar rapidamente *links* para várias ferramentas e sites relevantes. É uma maneira conveniente de ter acesso rápido a uma variedade de recursos de OSINT em um só lugar.

Ambos são plataformas online que reúnem uma variedade de ferramentas e recursos, proporcionando uma maneira conveniente e organizada de acessar informações e realizar investigações cibernéticas.

Embora a OSINT e HUMINT ofereçam uma ampla gama de possibilidades para a obtenção de informações relevantes, elas também possuem limitações e desafios a serem considerados. Ao longo deste estudo algumas limitações foram vivenciadas e catalogadas, tais como:

a) Manipulação de dados: a internet e as redes sociais possibilitam a disseminação rápida de informações, mas também facilitam a manipulação e o uso de desinformação. As informações coletadas através das técnicas exploradas neste artigo podem ser distorcidas ou alteradas para atender a determinadas agendas ou interesses;
b) Múltiplos contextos e níveis de informação: ao coletar informações de fontes diversas, pode ser difícil entender o contexto completo por trás dessas informações. A falta de contexto pode levar a interpretações equivocadas ou a uma compreensão superficial dos eventos;
c) Expressivo volume de informações: a quantidade massiva de dados disponíveis

gera uma sobrecarga de informações que pode dificultar a identificação de dados realmente úteis e valiosos;

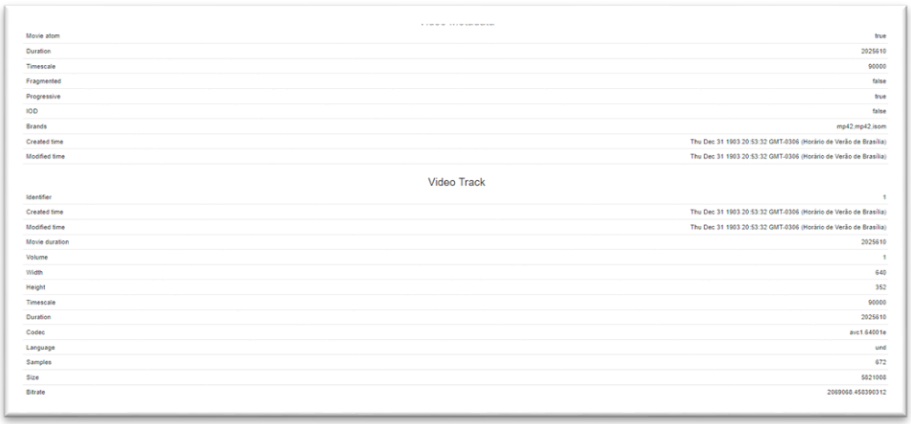
d) Complexidade das ferramentas: a habituação com as ferramentas é um aspecto crucial para o sucesso, uma vez que a vasta abundância de opções disponíveis pode ser esmagadora. Para identificar a ferramenta correta a ser utilizada em cada situação, é necessário ter uma experiência ampla e sólida no uso dessas ferramentas.

4 ESTUDO DE CASO

Neste capítulo será exposto um caso prático, onde foram utilizadas técnicas de HUMINT e OSINT para a relização da análise e conclusão. O caso prático consiste em um vídeo, que foi amplamente duvilgado no ano de 2023, em meio ao ambiente de ataques terroristas que aconteciam em escolas de diversos estados do Brasil. Este vídeo foi veiculado e divulgado como sendo, supostamente, um destes ataques.

Figura 1: *Frame* extraído do vídeo (objeto de análise)

Neste caso prático, o primeiro passo foi a fragmentação e extração de todos os *frames* que compoem o vídeo, desta forma, o segundo passo é a utilização de ferramentas de pesquisa reversa para localização de vídeos idênticos ou semelhantes. Para isso, pode-se utilizar a ferramenta *FakeNews DeBunker* e as pesquisas reversas das plataformas *Google*, *Yandex* e *Tineye*. Os resultados desta investida inicial não trouxeram informações suficientemente relevantes. Outro ponto que se é possível observar são os metadados do vídeo, que podem ser observados na ferramenta *FakeNews Debunker*.



Movie atom	true
Duration	2025610
Timescale	90000
Fragmented	false
Progressive	true
IOD	false
Brands	mp42:mp42:isom
Created time	Thu Dec 31 1903 20:53:32 GMT-0306 (Horário de Verão de Brasília)
Modified time	Thu Dec 31 1903 20:53:32 GMT-0306 (Horário de Verão de Brasília)

Video Track

Identifier	1
Created time	Thu Dec 31 1903 20:53:32 GMT-0306 (Horário de Verão de Brasília)
Modified time	Thu Dec 31 1903 20:53:32 GMT-0306 (Horário de Verão de Brasília)
Movie duration	2025610
Volume	1
Width	640
Height	352
Timescale	90000
Duration	2025610
Codec	avc1.64001e
Language	und
Samples	672
Size	5821008
Bitrate	2069068.450390312

Figura 2: Metadados extraídos do vídeo

Ao examinar cuidadosamente os *frames* observando as imagens de fundo, é possível identificar elementos que se assemelham à fachada de uma loja. Além disso, a presença de várias pessoas no local, vestindo roupas de diferentes empresas e estilos distintos, suscita a suspeita de que se trata de um local de acesso público frequente, possivelmente relacionado a estabelecimentos comerciais varejistas, como shoppings e supermercados. Essas indicações sugerem que a probabilidade maior seja a de ser um supermercado, dado que alguns *frames* exibem cestos de compras e uma pessoa segurando uma sacola.

Figura 3: *Frames* que mostram elementos em destaque

Desta forma, aplica-se a abordagem de pesquisa em motor de busca (*Google*) seguindo o seguinte parâmetro: intext=’atentado supermercado’. O retorno desta busca nos levou a uma postagem na rede social *Facebook*, que referenciava ao título: “Autor de explosão em supermercado de MT é preso” [6]. Retornando aos motores de busca e pesquisando por atentados a supermercados, foi encontrado a seguinte matéria no veículo de informação G1: Autor de explosão em supermercado de MT é preso e diz à polícia que tentou chantagear a empresa [7]. Também foi localizado no veículo Hora do Povo a seguinte matéria: Atentado a bomba de bolsonarista em Rondonópolis deixou uma criança gravemente ferida [8]. Tendo como base estas matérias, pode-se verificar a suspeita de que o susposto vídeo pode ter se passado na localização de Rondonópolis no estado de Mato Grosso.

Pesquisando em redes sociais por “atentado rondonópolis”, por datas retrospectivas a atual, foi possível localizar as publicações com o vídeo de origem na rede *Twitter* [9]. Essa descoberta reforça a suspeita de que o vídeo no contexto analisado é falso, possivelmente criado para gerar sensacionalismo ou desinformação.

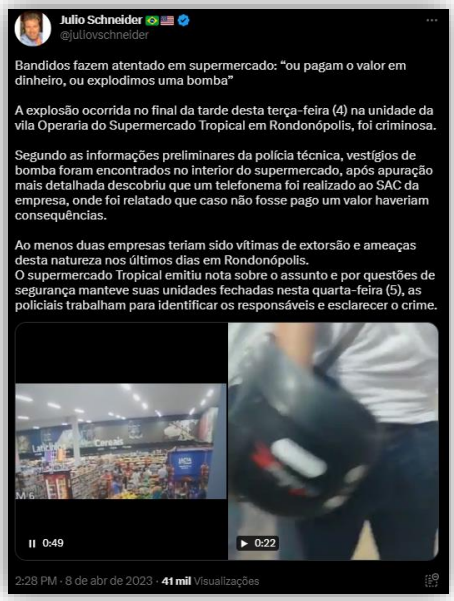


Figura 4: Publicação original na rede social *Twitter*

Diante dessas evidências apresentadas, após uma análise minuciosa das informações disponíveis, pode-se concluir, de forma definitiva, que o vídeo em questão não retrata um atentado relacionado aos ataques as escolas, ocorridos em março/abril de 2023. Em vez disso, o vídeo parece ser proveniente de um atentado que ocorreu em uma data diferente e em um contexto distinto. Essa conclusão é fundamentada na pesquisa realizada em motores de busca com auxilio das ferramentas utilizadas, onde podem ser observadas informações contraditórias às circunstâncias específicas dos ataques às escolas mencionados.

5 CONSIDERAÇÕES FINAIS

Em suma, este artigo destacou a capacidade e eficácia das técnicas de OSINT e HUMINT no contexto da inteligência cibernética. Além disso, demonstrou-se que a combinação dessas abordagens resulta em conquistas ainda mais promissoras, apesar dos desafios adicionais enfrentados. Por fim, foram aplicados os conceitos estudados a um caso prático, permitindo-nos observar, mesmo que de forma simulada, a aplicação real de todo o conhecimento exposto. Essa análise abrangente ressalta a importância dessas técnicas no campo da inteligência cibernética e evidencia seu potencial para contribuir de maneira significativa para a segurança e proteção digital. À medida que o cenário da tecnologia continua a evoluir, a adoção estratégica dessas abordagens se torna cada vez mais crucial para enfrentar os desafios emergentes. Portanto, é fundamental que organizações e profissionais da área estejam conscientes dessas técnicas e saibam como integrá-las de forma eficiente em suas operações de inteligência cibernética. A investigação e o aprimoramento contínuos dessas técnicas são fundamentais para acompanhar o panorama em constante mudança das ameaças digitais, fortalecendo assim a postura defensiva e possibilitando uma resposta eficaz a potenciais ataques cibernéticos.

REFERÊNCIAS

[1] Garcia, I. R. G: Humint e Osint na Era da Informação: a vantagem competitiva da Humint num mundo dominado por informação em acesso aberto. ISCSP-Universidade de Lisboa, janeiro 2020.

[2] Wendt, E: CIBERGUERRA, INTELIGÊNCIA CIBERNÉTICA E SEGURANÇA VIRTUAL: alguns aspectos. Revista Brasileira de Inteligência, abril 2011.

[3] Bamford, G; Felker, J; Mattern, T: Operational levels Of Cyber intelligence - Intelligence and national Security alliance. Cyber IntellIgence task Force, setembro 2013.

[4] Galindo, J, P; Pantaleone, N; Mármol, F, G; Pérez, G, M: The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. University of Murcia, janeiro 2020.

[5] Tabatabaei, F; Wells, D: OSINT in the Context of Cyber-Security. Springer International Publishing, 2016.

[6] Facebook [rede social na internet]: Autor de explosão em supermercado de MT é preso. Disponível em: https://www.facebook.com/watch/?v=1598040237366322, acesso em 05/2023.

[7] Portal G1 [homepage na Internet]: Autor de explosão em supermercado de MT é preso e diz à polícia que tentou chantagear a empresa. Disponível em: https://g1.globo.com/mt/mato-grosso/noticia/2023/04/12/autor-de-explosao-em-supermercado-de-mt-e-preso-e-diz-a-policia-que-tentou-chantagear-a-empresa.ghtml

[8] Portal Hora do Povo [homepage na Internet]: Atentado a bomba de bolsonarista em Rondonópolis deixou uma criança gravemente ferida. Disponível em: https://horadopovo.com.br/atentado-a-bomba-de-bolsonarista-em-rondonopolis-deixou-uma-crianca-gravemente-ferida/

[9] Twitter [rede social na internet]: Bandidos fazem atentado em supermercado. Disponível em: https://twitter.com/juliovschneider/status/1644753982835810305, acesso em 05/2023.