Large Language Models (LLMs) Aplicados à Atividade de Inteligência Militar

Sidnei Barbieri, Osmany Barros de Freitas e Lourenço Alves Pereira Júnior
Instituto Tecnológico de Aeronáutica - ITA

Resumo — A atividade de Inteligência Militar depende da consolidação, integração e análise de dados de diversas fontes, desde informações públicas até dados sensíveis. Este projeto propõe uma arquitetura integrada para coleta, análise e validação de dados, utilizando *Large Language Models* (LLMs) e agentes cognitivos para otimizar a análise de ativos e a produção de conhecimentos em proveito das operações de inteligência militar. A arquitetura inclui coleta autônoma de dados por *crawlers*, armazenamento em *Data Pool* e análises assistidas por LLMs. Resultados preliminares demonstram a viabilidade da arquitetura e a eficácia dos LLMs na consolidação e análise de dados em proveito da Inteligência Militar.

I. INTRODUÇÃO

A complexidade crescente das ameaças à Segurança e à Defesa Nacional exige uma abordagem integrada e sistemática para a coleta e análise de dados. As operações de inteligência militar modernas devem abranger uma variedade de fontes de dados, desde informações publicamente disponíveis na internet até dados sensíveis de fontes restritas [1]. O avanço tecnológico e o aumento exponencial na geração de dados intensificam essa necessidade. O uso de dados abertos tem sido uma prática comum na coleta de informações de inteligência, mas integrar esses dados com fontes como dispositivos comprometidos e sensores especializados apresenta desafios significativos em termos de integração, velocidade de atualização, verificação de credibilidade das fontes e segurança das informações [2].

A rápida evolução das tecnologias digitais e sua aplicação em operações militares aumentam os riscos à segurança dos ativos militares. Métodos avançados de análise de dados fornecem novas soluções para mitigar esses riscos. Assim LLMs emergem como ferramentas eficazes para aprimorar a inteligência de dados, combinando aprendizado semi-supervisionado e abordagens generativas para acelerar a interpretação de dados de *Open Source Intelligence* (OSINT) [3]. LLMs processam grandes volumes de texto e identificam padrões sutis, sendo essenciais para a identificação e análise de ativos militares, além da otimização de recursos e de efeitos em ações ofensivas [4]. Este projeto desenvolve uma plataforma integrada utilizando LLMs para melhorar a coleta, análise e validação de dados em operações de inteligência militar, focando na identificação e análise de ativos e na otimização de recursos e de efeitos em ações ofensivas [5].

II. ARQUITETURA

A plataforma unificada de inteligência de dados militar é composta pelas etapas ilustradas na Figura 1. A coleta de dados é realizada por *crawlers* autônomos e pela integração de múltiplas fontes. Os dados coletados são armazenados em um *Data Pool* (repositório central de dados brutos) para fins de auditoria e controle, preservando os dados originais. Uma cópia dos dados é processada para os objetivos finalísticos, sendo possível recorrer aos LLMs para processamento de texto a qualquer momento, indicando que todo o processo pode ser assistido por LLMs. A principal contribuição dos LLMs está na análise dos dados, incluindo escrutínio e validação, que abrange quatro etapas: análise de credibilidade, análise de contexto, comitês de análise e desenvolvimento de estratégias. A visualização dos dados é feita através de templates ou dashboards personalizados para diferentes níveis de comando. A plataforma inclui módulos de preparação e seleção de fontes de dados, onde a interação humana é necessária para catalogação, estratégia de acesso, confirmação de autenticidade e análise de pertinência. Desta forma, o uso de LLMs visa melhorar a coleta, análise e validação dos dados em operações de inteligência militar, focando na identificação e análise de ativos e na otimização de recursos e efeitos em ações ofensivas.

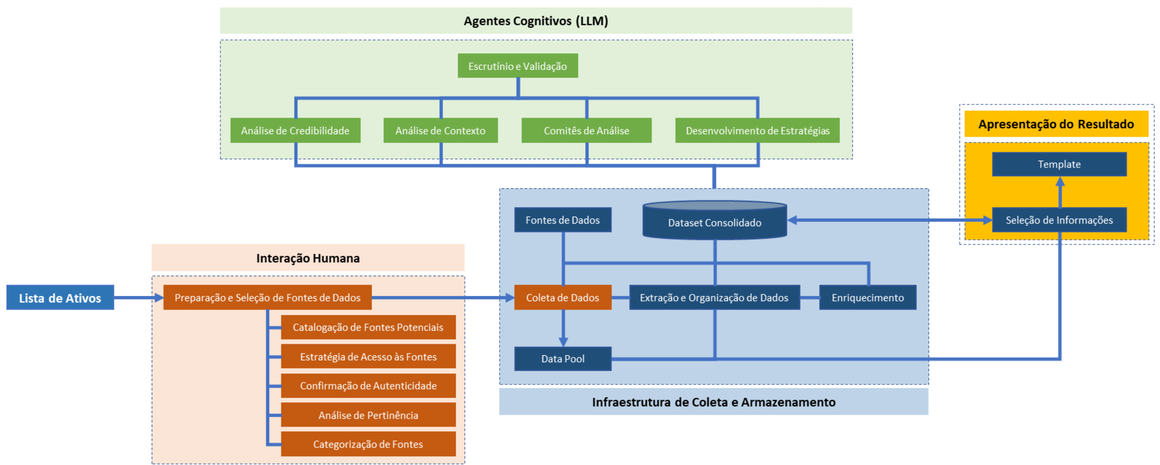


Figura 1. Arquitetura integrada de LLM para coleta e análise de dados em inteligência militar.

III. INTERAÇÃO HUMANA

Este módulo permite a coleta autônoma de dados a partir de fontes predefinidas, necessitando de interação humana inicial. A arquitetura modular permite a integração eficiente de novos componentes e fontes de dados, incluindo a incorporação de novos crawlers e a adaptação às mudanças nas fontes de dados existentes, abrangendo desde fontes abertas até sistemas restritos. A preparação e seleção de fontes de dados, assim como a definição da estratégia de coleta, requerem interação humana para catalogação, estratégia de acesso, confirmação de autenticidade, análise de pertinência e categorização. Após essa etapa inicial, a coleta de dados é automatizada e o processo de extração e análise pode ser assistido ou apoiado por LLMs, minimizando a dependência da intervenção humana. Esse processo garante que as fontes são relevantes e aumentam a confiabilidade dos dados para a inteligência militar.

IV. INFRAESTRUTURA DE COLETA E ARMAZENAMENTO

Este módulo é centralizado em um *Data Pool*, que permite o armazenamento de dados heterogêneos em grande escala. Os *crawlers* autônomos realizam a coleta de dados de diversas fontes, armazenando essas informações diretamente no *Data Pool*. Este *Data Pool* é capaz de lidar com a diversidade e o volume de dados necessários para operações militares, favorecendo a análise e a tomada de decisões baseadas em dados [6]. A infraestrutura implementa a automação da coleta, extração e organização dos dados por meio dos *crawlers*, além do enriquecimento através de técnicas de limpeza e integração. Esta infraestrutura assegura que os dados são coletados, organizados e armazenados de forma eficiente e segura, prontos para a análise aprofundada, automatizada com a assistência dos LLMs.

V. AGENTES COGNITIVOS

Os agentes cognitivos analisam e interpretam os dados, validando a integridade e relevância, avaliando a credibilidade das fontes e analisando o contexto dos dados para melhor interpretação. O uso de LLMs para auxiliar na avaliação da credibilidade dos dados coletados via OSINT está ganhando atenção crescente [7]. Estudos têm demonstrado que a incorporação de sinais de credibilidade em modelos de geração de respostas pode mitigar a propagação de desinformação e melhorar a qualidade das decisões informadas por esses dados [8]. O processo de escrutínio e validação é dividido em quatro etapas: análise de credibilidade, análise de contexto, comitês de análise e desenvolvimento de estratégias. Agentes cognitivos com LLMs operam de forma automatizada, simulando times revisores e validadores de dados.

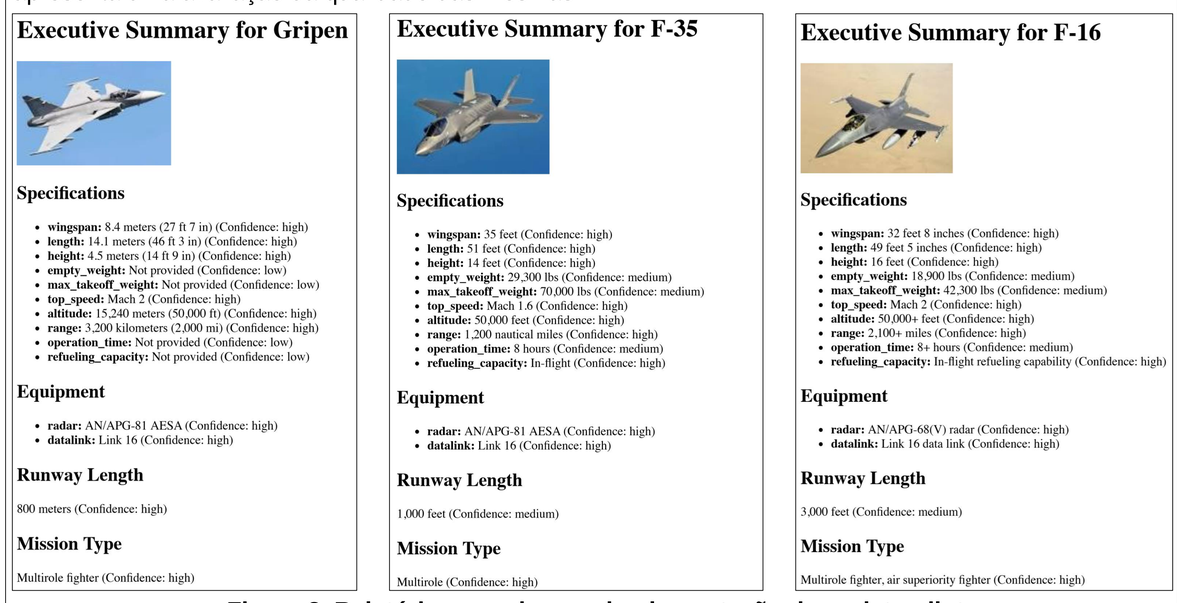
Os *insights* gerados são utilizados para desenvolver estratégias de defesa e ação. É importante considerar o *feedback* operacional nesse processo, visando aprimorar continuamente os modelos e a metodologia. Essa integração visa ampliar a precisão e agregar valor às análises no âmbito da inteligência em operações militares, com o objetivo de respeitar a privacidade e segurança dos dados.

VI. APRESENTAÇÃO DO RESULTADO

Os resultados são apresentados em *templates* padronizados, com as informações mais relevantes selecionadas para atender aos interesses dos diferentes públicos-alvos ou níveis de comando. Quando integrada, a plataforma oferece a flexibilidade de gerar sumários executivos, slides ou dashboards, aprimorando a visualização dos dados e a comunicação dos *insights* gerados. Isso contribui para um planejamento tático, operacional e estratégico mais ágil, fundamentado em um vasto conjunto de informações previamente avaliadas quanto à qualidade.

VII. RESULTADOS PRELIMINARES

Para validar a arquitetura proposta, foi implementado um projeto piloto em linguagem R, contemplando uma versão minimalista da estrutura. Os dados brutos das fontes são armazenados no *Data Pool* para verificações, como validação e auditoria. Esses dados são processados e refinados, resultando em arquivos JSON armazenados no diretório *assets*. Esses arquivos refinados são utilizados como base de dados estruturada para gerar os sumários executivos. A simulação dos agentes cognitivos foi realizada utilizando o modelo ChatGPT, operando de forma autônoma, sem intervenção humana. Os experimentos preliminares demonstraram a viabilidade da arquitetura proposta. Foram gerados três relatórios técnicos sobre as aeronaves "Gripen," "F-16" e "F-35“, Figura 2, utilizando dados de fontes abertas, incluindo *Wikipedia*, *GlobalSecurity.org* e *Google Images*. Além disso, foi empregado o modelo ChatGPT-3.5 Turbo, acessado via API, como uma fonte adicional de baixo custo devido à sua extensa base de dados. Esses relatórios contêm especificações e informações técnicas, facilmente convertidas em análises de nível tático, operacional ou estratégico. Assim, o experimento demonstrou a capacidade do sistema de consolidar e analisar dados de forma eficiente e, embora compatíveis com a qualidade das fontes, também apresenta uma avaliação da qualidade das mesmas.



Executive Summary for Gripen

Specifications

- **wingspan:** 8.4 meters (27 ft 7 in) (Confidence: high)
- **length:** 14.1 meters (46 ft 3 in) (Confidence: high)
- **height:** 4.5 meters (14 ft 9 in) (Confidence: high)
- **empty_weight:** Not provided (Confidence: low)
- **max_takeoff_weight:** Not provided (Confidence: low)
- **top_speed:** Mach 2 (Confidence: high)
- **altitude:** 15,240 meters (50,000 ft) (Confidence: high)
- **range:** 3,200 kilometers (2,000 mi) (Confidence: high)
- **operation_time:** Not provided (Confidence: low)
- **refueling_capacity:** Not provided (Confidence: low)

Equipment

- **radar:** AN/APG-81 AESA (Confidence: high)
- **datalink:** Link 16 (Confidence: high)

Runway Length

800 meters (Confidence: high)

Mission Type

Multirole fighter (Confidence: high)

Executive Summary for F-35

Specifications

- **wingspan:** 35 feet (Confidence: high)
- **length:** 51 feet (Confidence: high)
- **height:** 14 feet (Confidence: high)
- **empty_weight:** 29,300 lbs (Confidence: medium)
- **max_takeoff_weight:** 70,000 lbs (Confidence: medium)
- **top_speed:** Mach 1.6 (Confidence: high)
- **altitude:** 50,000 feet (Confidence: high)
- **range:** 1,200 nautical miles (Confidence: high)
- **operation_time:** 8 hours (Confidence: medium)
- **refueling_capacity:** In-flight (Confidence: high)

Equipment

- **radar:** AN/APG-81 AESA (Confidence: high)
- **datalink:** Link 16 (Confidence: high)

Runway Length

1,000 feet (Confidence: medium)

Mission Type

Multirole (Confidence: high)

Executive Summary for F-16

Specifications

- **wingspan:** 32 feet 8 inches (Confidence: high)
- **length:** 49 feet 5 inches (Confidence: high)
- **height:** 16 feet (Confidence: high)
- **empty_weight:** 18,900 lbs (Confidence: medium)
- **max_takeoff_weight:** 42,300 lbs (Confidence: medium)
- **top_speed:** Mach 2 (Confidence: high)
- **altitude:** 50,000+ feet (Confidence: high)
- **range:** 2,100+ miles (Confidence: high)
- **operation_time:** 8+ hours (Confidence: medium)
- **refueling_capacity:** In-flight refueling capability (Confidence: high)

Equipment

- **radar:** AN/APG-68(V) radar (Confidence: high)
- **datalink:** Link 16 data link (Confidence: high)

Runway Length

3,000 feet (Confidence: medium)

Mission Type

Multirole fighter, air superiority fighter (Confidence: high)

Figura 2. Relatórios gerados por implementação de projeto piloto

VIII. CONCLUSÃO

Entre os desafios enfrentados, destacam-se o tratamento de fontes de dados heterogêneas e a avaliação de sua qualidade. Nesta primeira fase, evitou-se a utilização de fontes reconhecidas disponíveis apenas mediante pagamento. Além disso, não foi aprofundada a avaliação de estratégias automatizadas para o escrutínio e validação dos dados. Essas questões foram mitigadas por meio de *scripts* R assistidos por LLMs, simplificando os processos de análise e avaliação da credibilidade das informações. A utilização de *scripts* R em substituição à infraestrutura completa reduziu o tempo necessário para o início dos experimentos, validando o projeto e destacando a eficiência e a robustez da arquitetura proposta. Os resultados obtidos demonstram a viabilidade e o potencial da solução proposta que utiliza LLMs aplicados à atividade de Inteligência Militar.

REFERÊNCIAS

1. SCHULZE, Matthias. Cyber in war: Assessing the strategic, tactical, and operational utility of military cyber operations. In: 2020 12th International Conference on Cyber Conflict (CyCon). IEEE, 2020. p. 183-197.
2. LILLY, Bilyana; CHERAVITCH, Joe. The past, present, and future of Russia’s cyber strategy and forces. In: 2020 12th International Conference on Cyber Conflict (CyCon). IEEE, 2020. p. 129-155.
3. SIRACUSANO, Giuseppe et al. Time for action: Automated analysis of cyber threat intelligence in the wild. arXiv preprint arXiv:2307.10214, 2023.
4. FERRAG, Mohamed Amine et al. Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for iot/iiot devices. IEEE Access, 2024.
5. CHERQI, Othmane et al. Enhancing cyber threat identification in open-source intelligence feeds through an improved semi-supervised generative adversarial learning approach with contrastive learning. IEEE Access, 2023.
6. HAI, Rihan; GEISLER, Sandra; QUIX, Christoph. Constance: An intelligent data lake system. In: Proceedings of the 2016 international conference on management of data. 2016. p. 2097-2100.
7. LEITE, João A. et al. Detecting misinformation with llm-predicted credibility signals and weak supervision. arXiv preprint arXiv:2309.07601, 2023.
8. PAN, Ruotong et al. Not All Contexts Are Equal: Teaching LLMs Credibility-aware Generation. arXiv preprint arXiv:2404.06809, 2024.