ANÁLISE PREDITIVA DE ATAQUES CIBERNÉTICOS USANDO REDES NEURAIS

Wenderson Luiz Portela da Silva[1]

[1]Universidade Federal de Sergipe – UFS / wendersonportela1@gmail.com

Resumo

O uso de técnicas de redes neurais tem se consolidado como um recurso estratégico na segurança cibernética, oferecendo novas abordagens para a análise preditiva de ataques, a detecção de intrusões e a antecipação de ameaças digitais. Este estudo apresenta uma revisão sistemática da literatura, contemplando sete artigos publicados entre 2021 e 2025 e selecionados no Google Acadêmico, que discutem aplicações de modelos de aprendizado profundo e incremental em diferentes contextos de cibersegurança. Os resultados evidenciam que as redes neurais contribuem para aprimorar a precisão na identificação de padrões maliciosos, reduzir taxas de falsos positivos em sistemas de detecção de intrusão, classificar tráfego de rede com maior eficiência e apoiar estratégias de defesa proativa contra ataques cibernéticos. Apesar dos avanços, a literatura também aponta desafios relevantes, como a necessidade de bases de dados balanceadas e representativas, a mitigação de problemas de esquecimento catastrófico em modelos incrementais, além das limitações relacionadas ao custo computacional e à escalabilidade em ambientes de produção. A contribuição deste estudo consiste em sintetizar evidências recentes sobre o tema, oferecendo subsídios para o desenvolvimento de soluções preditivas mais robustas, eficazes e alinhadas às demandas contemporâneas de segurança digital.

Palavras-chave: Análise preditiva. Ataques cibernéticos. Redes neurais.

Introdução

A intensificação da transformação digital tem ampliado significativamente a superfície de ataque no ciberespaço, tornando a segurança da informação um dos maiores desafios contemporâneos. A sofisticação das ameaças digitais, como ataques de *ransomware*, negação de serviço distribuída (DDoS) e intrusões avançadas, exige soluções que vão além da simples detecção reativa. Nesse contexto, técnicas de inteligência artificial, em especial as redes neurais, têm se consolidado como alternativas promissoras para a análise preditiva de ataques cibernéticos.

O uso de algoritmos de aprendizado de máquina supervisionado e não supervisionado já se mostrou eficaz na classificação de tráfego e na detecção de intrusões, conforme discutido por Martins *et al*. (2024), que destacam ganhos relevantes em acurácia e redução de falsos positivos em sistemas de detecção de ataques. De forma complementar, Pereira Filho (2023)

apresenta um estudo de viabilidade sobre a adoção de modelos preditivos de ataques em redes de computadores, ressaltando tanto o potencial dessas abordagens quanto os desafios associados à implementação em ambientes reais. Nesse mesmo sentido, Lacerda (2023) amplia a discussão para o contexto brasileiro de cibercrime, destacando como a inteligência artificial, em especial as redes neurais, pode contribuir para estratégias de prevenção e fortalecimento das práticas de segurança digital no país.

Entre os avanços recentes, destaca-se o trabalho de Lemos *et al*. (2024), que propõem o uso de aprendizado incremental para sistemas de detecção de intrusão, mitigando o problema do esquecimento catastrófico em ambientes dinâmicos de segurança. De forma convergente, Bona e Leal (2024) discutem a integração de arquiteturas cognitivas, inteligência artificial e ambientes *cloud-native*, reforçando a necessidade de soluções escaláveis e adaptáveis para cenários complexos de cibersegurança.

Outra vertente importante é explorada por Moura (2023), que utiliza gêmeos digitais (*digital twins*) para o monitoramento de infraestruturas críticas, demonstrando como essa tecnologia, aliada a modelos de aprendizado de máquina, pode antecipar falhas e identificar potenciais ataques cibernéticos. Da mesma forma, estudos como o de Silva *et al*. (2023) analisam aplicações de redes neurais em diferentes contextos de segurança digital, abordando desde mecanismos de autenticação até estratégias de mitigação de fraudes.

Apesar dos progressos, a literatura converge em apontar desafios recorrentes, como a necessidade de bases de dados representativas, o elevado custo computacional dos modelos mais complexos, os vieses algorítmicos e a dificuldade de escalar soluções em ambientes produtivos (Martins *et al*., 2024; Lemos *et al*., 2024; Pereira Filho, 2023).

Diante desse cenário, este trabalho tem como objetivo realizar uma revisão sistemática da literatura sobre o uso de redes neurais na análise preditiva de ataques cibernéticos, a partir de sete artigos publicados entre 2021 e 2025 no Google Acadêmico. Busca-se identificar metodologias aplicadas, resultados alcançados, principais desafios relatados e tendências futuras, contribuindo para o fortalecimento de pesquisas e práticas na área de segurança cibernética.

Metodologia

Este estudo foi conduzido por meio de uma revisão sistemática da literatura, com base nas diretrizes do PRISMA 2020, a fim de identificar e analisar as principais contribuições do uso de redes neurais na análise preditiva de ataques cibernéticos. O processo metodológico

envolveu quatro etapas principais: definição dos critérios de elegibilidade, busca e seleção dos artigos, extração de dados e síntese dos resultados.

Os critérios de inclusão abrangeram artigos publicados entre 2021 e 2025, em língua portuguesa ou inglesa, que abordassem de forma empírica ou analítica a aplicação de redes neurais em mecanismos de análise preditiva voltados à segurança cibernética. Foram excluídos trabalhos duplicados, artigos fora do período definido e estudos que, embora utilizassem termos relacionados, não apresentavam vínculo direto com o tema investigado.

A busca foi realizada no Google Acadêmico utilizando a combinação de descritores em português: “análise preditiva” *AND* “ataques cibernéticos” *AND* “redes neurais”. Essa estratégia resultou na identificação inicial de diversos estudos, dos quais sete artigos foram selecionados após a leitura dos títulos, resumos e textos completos, por atenderem aos critérios previamente estabelecidos (Lemos *et al*., 2024; Bona; Leal, 2024; Martins *et al*., 2024; Silva *et al*., 2023; Pereira Filho, 2023; Moura, 2023; Lacerda, 2023).

A extração dos dados foi realizada por meio da elaboração de uma matriz contendo informações sobre: autores, ano de publicação, objetivos, técnicas de redes neurais empregadas, bases de dados utilizadas, principais resultados obtidos e limitações apontadas.

A síntese dos achados foi conduzida de forma narrativa, agrupando os estudos de acordo com suas contribuições, benefícios e desafios relacionados ao uso de modelos neurais em segurança cibernética, especialmente em tarefas de detecção de intrusão, classificação de tráfego malicioso e antecipação de ameaças digitais.

Essa abordagem metodológica permite sistematizar e interpretar criticamente a produção científica recente sobre o tema, contribuindo para a identificação de tendências emergentes, lacunas ainda existentes e direcionamentos para futuras pesquisas na área de segurança cibernética com suporte de inteligência artificial.

Resultados e discussões

O uso de redes neurais na análise preditiva de ataques cibernéticos tem sido amplamente explorado nos últimos anos, com diferentes enfoques metodológicos e aplicações práticas. A literatura recente revela esforços tanto no desenvolvimento de novos modelos quanto na adaptação de arquiteturas existentes para contextos de segurança digital.

Lemos *et al*. (2024) discutem a aplicação de aprendizado incremental em sistemas de detecção de intrusão, buscando mitigar o problema do esquecimento catastrófico em modelos neurais. A proposta mostrou-se eficaz em cenários dinâmicos, possibilitando que os sistemas

de segurança mantenham desempenho estável mesmo diante da constante evolução dos padrões de ataque.

De forma complementar, Bona e Leal (2024) enfatizam a importância da integração entre arquiteturas cognitivas e ambientes *cloud-native*, destacando que soluções baseadas em redes neurais necessitam não apenas de alta acurácia, mas também de escalabilidade e adaptabilidade. Os autores sugerem que a adoção de infraestruturas distribuídas potencializa o uso da inteligência artificial em ambientes de produção.

Em linha semelhante, Martins *et al*. (2024) apresentam um estudo que compara abordagens de aprendizado supervisionado e não supervisionado para a detecção de ataques, demonstrando que as redes neurais oferecem ganhos significativos na classificação de tráfego malicioso, principalmente na redução de falsos positivos.

Outro trabalho relevante é o de Pereira Filho (2023), que realiza um *survey* sobre modelos preditivos de ataques em redes de computadores, abordando desde arquiteturas neurais até algoritmos híbridos. O estudo reforça a viabilidade das técnicas preditivas, mas aponta limitações quanto à generalização dos modelos e à necessidade de bases de dados mais representativas.

Já Moura (2023) explora a utilização de gêmeos digitais (*digital twins*) no monitoramento de infraestruturas críticas, combinando a modelagem virtual de sistemas com técnicas de aprendizado de máquina. Os resultados indicam que a estratégia pode antecipar falhas e detectar indícios de ataques cibernéticos em tempo real, ampliando a capacidade de defesa preventiva.

Além disso, Silva *et al*. (2023) abordam aplicações de redes neurais em diferentes contextos de segurança cibernética, incluindo autenticação, prevenção de fraudes e monitoramento de sistemas distribuídos. O estudo evidencia a versatilidade dessas técnicas, mas ressalta a necessidade de modelos mais leves para implantação em dispositivos de borda.

No contexto brasileiro, Lacerda (2023) discute a utilização da inteligência artificial como instrumento de prevenção ao cibercrime, enfatizando a importância de soluções baseadas em redes neurais para antecipar ataques e reduzir vulnerabilidades em sistemas nacionais. Sua análise contribui para destacar não apenas o caráter tecnológico das abordagens, mas também a relevância social e jurídica do emprego de técnicas preditivas em segurança digital.

Por fim, outros trabalhos incluídos na revisão reforçam os desafios comuns à área, como o alto custo computacional de arquiteturas profundas, a dependência de conjuntos de

dados balanceados, e a dificuldade de escalar soluções experimentais para ambientes reais de produção.

De forma geral, a revisão evidencia que as redes neurais têm desempenhado papel central na evolução da cibersegurança preditiva, mas ainda carecem de avanços em termos de eficiência, interpretabilidade e robustez para consolidarem seu uso em larga escala.

Considerações Finais

A revisão sistemática realizada permitiu identificar e analisar as principais contribuições recentes sobre o uso de redes neurais na análise preditiva de ataques cibernéticos, a partir de sete estudos publicados entre 2021 e 2025. Os resultados apontam que essas técnicas vêm se consolidando como ferramentas estratégicas na detecção de intrusões, classificação de tráfego malicioso e antecipação de ameaças digitais, além de contemplar discussões específicas sobre o cenário brasileiro de cibercrime, como apresentado por Lacerda (2023), que ressalta o papel da inteligência artificial como aliada na prevenção de ataques.

Entre os avanços destacados, ressaltam-se as propostas de aprendizado incremental para superar o esquecimento catastrófico, a integração de arquiteturas cognitivas e ambientes *cloud-native*, bem como a aplicação de gêmeos digitais no monitoramento de infraestruturas críticas. Esses trabalhos demonstram a diversidade de abordagens em desenvolvimento e o potencial das redes neurais como suporte a estratégias de defesa proativa em segurança cibernética.

Apesar disso, a literatura revisada converge na indicação de desafios que ainda limitam a consolidação dessas soluções em larga escala. Questões como a dependência de bases de dados amplas e representativas, o alto custo computacional de arquiteturas profundas, a mitigação de vieses algorítmicos e a escalabilidade em ambientes produtivos permanecem como barreiras relevantes a serem superadas.

Nesse sentido, pesquisas futuras devem explorar modelos neurais mais leves e interpretáveis, capazes de serem implementados em dispositivos de borda com baixo custo computacional; estratégias híbridas que combinem aprendizado supervisionado, não supervisionado e incremental; além do desenvolvimento de conjuntos de dados padronizados e diversificados, que representem melhor os cenários reais de ataques. Outra vertente promissora envolve o avanço de técnicas de *eXplainable* AI (XAI) aplicadas à segurança, de forma a aumentar a confiabilidade das decisões automatizadas em contextos críticos.

Assim, este estudo contribui para sintetizar o estado da arte sobre o tema, oferecendo subsídios para a evolução de soluções de segurança digital mais robustas, escaláveis e alinhadas às demandas contemporâneas da sociedade conectada.

Referências

BONA, R.; LEAL, R. Arquiteturas cognitivas e ambientes *cloud-native*: desafios e oportunidades para a segurança cibernética. **Revista de Iniciação Científica em Computação**, v. 22, n. 2, p. 45-59, 2024.

LACERDA, Talles Barbosa de. **Cibercrime no Brasil**: a utilização da inteligência artificial como possibilidade de prevenção. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Centro Universitário Doutor Leão Sampaio (Unileão), 2023.

LEMOS, A. R.; OLIVEIRA, F. A.; SANTOS, J. P. Aprendizado incremental para detecção de intrusão: uma abordagem para mitigar o esquecimento catastrófico. **Anais do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)**, 2024.

MARTINS, G. H.; SOUZA, P. C.; ALMEIDA, V. R. Redes neurais aplicadas à detecção de ataques: estudo comparativo entre aprendizado supervisionado e não supervisionado. **Revista de Sistemas e Computação,** v. 34, n. 1, p. 101-118, 2024.

MOURA, L. S. Uso de gêmeos digitais para monitoramento de infraestruturas críticas: aplicações em segurança cibernética. **Journal of Information Security and Digital Forensics**, v. 12, n. 3, p. 87-99, 2023.

PEREIRA FILHO, C. Modelos preditivos de ataques em redes de computadores: um estudo de viabilidade. **Revista de Engenharia e Tecnologia Aplicada**, v. 15, n. 1, p. 25-40, 2023.

SILVA, M. J.; COSTA, R. F.; ANDRADE, L. M. Aplicações de redes neurais em segurança digital: autenticação, prevenção de fraudes e monitoramento distribuído. **Anais da Conferência Nacional de Inteligência Artificial e Segurança da Informação (CONIASI)**, 2023.