Eixo temático: Prevenção contra Crimes Cibernéticos

DA AMEAÇA À PROTEÇÃO: A GUERRA DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA CIBERNÉTICA

Israel Lucas Lima Campos[1]; Álvaro Guilherme Barreto dos Santos[2] e Ronierison de Souza Maciel[3]

INTRODUÇÃO

A Inteligência Artificial (IA) deixou de ser um recurso tecnológico associado à inovação e passou a ocupar papel nas discussões sobre segurança da informação. Nos últimos anos, o avanço de algoritmos de aprendizado de máquina e redes neurais profundas tem permitido que máquinas não apenas processem grandes volumes de dados, mas também tomem decisões autônomas com base em padrões complexos. Esse cenário, que antes era restrito ao campo da pesquisa, atualmente encontra-se em setores estratégicos como saúde, economia, indústria, educação e, sobretudo, na cibersegurança.

No ambiente digital, a IA desempenha uma função paradoxal: enquanto fortalece os mecanismos de proteção, também é apropriada por agentes maliciosos para potencializar ataques. Hackers, por exemplo, têm utilizado sistemas inteligentes para criar ataques difíceis de detectar, como phishing hiperpersonalizado, deepfakes maliciosos e malwares autônomos capazes de se adaptar às barreiras de defesa (BUSTAMANTE, 2025). Por outro lado, empresas e governos recorrem a soluções baseadas em IA para monitorar redes em tempo real, detectar anomalias, bloquear conexões suspeitas e até mesmo prever vulnerabilidades antes que sejam exploradas (VOLPI, 2025; PUC-RIO, 2025).

Essa disputa caracteriza o que especialistas chamam de “guerra invisível” no ciberespaço (COMPUTER WEEKLY BRASIL, 2024). Diferente dos conflitos tradicionais, ela

[1] Bacharelando em Sistema de Informação, no Centro Universitário do Rio São Francisco – UniRios. E-mail: israellucascamposlima@gmail.com
[2] Bacharelando em Sistemas de Informação, no Centro Universitário do Rio São Francisco – UniRios.
[3] Mestre e doutorando na área de Ciência da Computação pela UFPE, docente do curso de Sistemas de Informação no Centro Universitário do Rio São Francisco – UniRios. E-mail: ronierison.maciel@unirios.edu.br

não ocorre em campos de batalha físicos, mas em ambientes digitais, onde algoritmos duelam silenciosamente para garantir a proteção ou o comprometimento de sistemas críticos. Essa nova forma de conflito traz desafios que extrapolam a esfera técnica, envolvendo também questões sociais, econômicas, éticas e políticas.

Diante disso, aumenta a preocupação com a crescente dependência da sociedade em sistemas digitais e com os riscos associados à utilização da IA sem regulamentação adequada. A desigualdade no acesso à cibersegurança torna pequenas organizações mais vulneráveis, enquanto os impactos sociais e jurídicos de ataques autônomos descontrolados exigem um debate amplo e aprofundado. A discussão, portanto, não se limita a especialistas em tecnologia, mas alcança toda a sociedade, uma vez que a segurança digital está diretamente ligada à proteção de dados pessoais, da infraestrutura crítica e até da soberania dos Estados.

Assim, este trabalho trata da análise da Inteligência Artificial como instrumento de ataque e defesa na segurança cibernética, destacando sua relevância para compreender os desafios e as oportunidades desse embate tecnológico. A importância do estudo está em evidenciar não apenas os riscos envolvidos, mas também as possibilidades de fortalecer mecanismos de defesa e fomentar debates sobre regulamentação, ética e equidade no acesso à proteção digital.

OBJETIVO

O presente trabalho tem como objetivo analisar o uso da Inteligência Artificial como instrumento de ataque e defesa na segurança cibernética**,** destacando exemplos práticos, riscos e perspectivas de mitigação dessa guerra tecnológica.

METODOLOGIA

Trata-se de uma pesquisa qualitativa, com caráter bibliográfico e exploratório, realizada a partir de artigos científicos, relatórios institucionais e matérias jornalísticas brasileiras e internacionais sobre o uso da IA na cibersegurança. O estudo analisou criticamente diferentes perspectivas na literatura, de modo a compreender como a Inteligência Artificial vem sendo aplicada tanto em ataques quanto em mecanismos de defesa digital.

Foram selecionadas fontes que descrevem estratégias ofensivas, como phishing: um estudo envolvendo foram selecionadas fontes que descrevem estratégias ofensivas, como phishing — em estudos envolvendo DeepSeek, Gemini e ChatGPT (BUSTAMANTE, 2025) — além de técnicas emergentes como *prompt injection*, que exploram instruções maliciosas para manipular modelos de linguagem. No campo defensivo, foram analisados sistemas XDR e métodos de análise preditiva (VOLPI, 2025; PUC-RIO, 2025). Essa abordagem qualitativa possibilitou não apenas a descrição dos fenômenos, mas também a interpretação de seus impactos sociais, econômicos e éticos, em consonância com os objetivos propostos pelo trabalho."

RESULTADOS E DISCUSSÕES

Os resultados apontam que a IA amplia significativamente o alcance e a sofisticação dos ataques digitais. O uso de deepfakes em fraudes e manipulações de imagem, que já representam sérios riscos à privacidade e à segurança jurídica (SIQUEIRA; ANDRADE, 2024), e campanhas de phishing generativo com mensagens praticamente indetectáveis (BUSTAMANTE, 2025) exemplificam a escalada de ameaças.

Por outro lado, as defesas baseadas em IA têm apresentado avanços significativos. Ferramentas como os sistemas XDR realizam o monitoramento contínuo e bloqueiam conexões maliciosas de forma automática, sem depender de intervenção humana (VOLPI, 2025; PUC-RIO, 2025). Além disso, a análise preditiva e a detecção de anomalias em tempo real mostram-se fundamentais para identificar e antecipar possíveis vulnerabilidades (PUC-RIO, 2025)."

No entanto, emergem desafios como a dependência excessiva dessas tecnologias (COMPUTER WEEKLY BRASIL, 2024) e a desigualdade no acesso a sistemas avançados de defesa, que afeta especialmente pequenas e médias empresas (NEUBER, 2025).

CONSIDERAÇÕES FINAIS

Conclui-se que a Inteligência Artificial ocupa um papel fundamental na cibersegurança: ao mesmo tempo em que se consolida como arma de ataque, também se firma como escudo de defesa. Esse embate redefine os limites da segurança digital e demonstra que a disputa entre

ofensiva e defensiva está em constante evolução, o que exige atenção permanente de especialistas, governos e empresas.

A análise evidencia que não basta apenas desenvolver tecnologias sofisticadas, mas garantir que elas sejam acompanhadas de regulamentações claras**,** políticas públicas eficazes e práticas éticas responsáveis, de modo a assegurar maior equidade no acesso à proteção tecnológica (GOVERNO DO BRASIL, 2025; ABRASECI, 2025; IBRINC, 2025). Sem tais medidas, corre-se o risco de ampliar desigualdades já existentes, deixando pequenas e médias organizações mais vulneráveis frente a grandes corporações que possuem recursos para investir em segurança digital avançada.

O futuro da cibersegurança, portanto, dependerá da capacidade de equilibrar inovação e responsabilidade, de modo que a IA não seja apenas instrumento de ameaça, mas também promotora de justiça e segurança digital. Além disso, é fundamental que a sociedade como um todo participe do debate sobre o uso ético dessas tecnologias, reconhecendo que a proteção de dados, da infraestrutura crítica e da soberania digital ultrapassa os limites técnicos e envolve dimensões sociais**,** políticas e jurídicas.

Somente por meio de uma abordagem multidisciplinar e colaborativa será possível transformar a IA em uma aliada da cibersegurança, fortalecendo não apenas sistemas e redes, mas também valores democráticos e a proteção da cidadania em meio ao avanço da era digital.

PALAVRAS-CHAVE

Cibersegurança. Defesa Cibernética. Deepfake. Inteligência Artificial. Phishing.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE SEGURANÇA CIBERNÉTICA (ABRASECI). **Associação Brasileira de Segurança Cibernética.** Wikipédia, 2025. Disponível em: https://pt.wikipedia.org/wiki/Associa%C3%A7%C3%A3o_Brasileira_de_Seguran%C3%A7a_Cibern%C3%A9tica. Acesso em: 25 ago. 2025.

BUSTAMANTE, Evelyn Estefania Bravo. ***Uma Metodologia Comparativa para Avaliação de LLMs na Detecção de Phishing****: Um Estudo Envolvendo DeepSeek, Gemini e ChatGPT*. 2025. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Universidade Federal de Uberlândia, Uberlândia, 2025. Disponível em: https://repositorio.ufu.br/handle/123456789/46058. Acesso em: 12 set. 2025.

COMPUTER WEEKLY BRASIL. **Um panorama abrangente da revolução da IA na segurança cibernética no Brasil.** Computer Weekly, 2024. Disponível em: https://www.computerweekly.com/br/reportagen/Um-panorama-abrangente-da-revolucao-da-IA-na-seguranca-cibernetica-no-Brasil. Acesso em: 25 ago. 2025.

GOVERNO DO BRASIL. **Segurança cibernética é discutida em encontro do SISBIN Nordeste.** Gov.br, 2025. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/seguranca-cibernetica-e-discutida-em-encontro-do-sisbin-nordeste. Acesso em: 25 ago. 2025.

INSTITUTO BRASILEIRO DE RESPOSTA A INCIDENTES CIBERNÉTICOS (IBRINC). **Instituto Brasileiro de Resposta a Incidentes Cibernéticos.** Wikipédia, 2025. Disponível em: https://pt.wikipedia.org/wiki/Instituto_Brasileiro_de_Resposta_a_Incidentes_Cibern%C3%A9ticos. Acesso em: 25 ago. 2025.

NEUBER, Diego. **Cybersegurança:** principais desafios enfrentados por pequenas e médias empresas**.** *Revista de Iniciação à Pesquisa Acadêmica*, v. 6, n. 27, p. 1-15, jan./jun. 2025. Universidade Norte do Paraná. Disponível em: https://periodicos.ufes.br/ipa/article/view/47085. Acesso em: 12 set. 2025.

PUC-RIO (CCEC). **IA e Cibersegurança:** como a Inteligência Artificial está revolucionando a proteção digital**.** CCEC – PUC-Rio, 2025. Disponível em: https://especializacao.ccec.puc-rio.br/blog/ia-ciberseguranca. Acesso em: 25 ago. 2025.

PROTIVITI. **Avanços e riscos da Inteligência Artificial na Cibersegurança.** Protiviti Brasil, 2025. Disponível em: https://www.protiviti.com.br/cybersecurity/avancos-e-riscos-da-inteligencia-artificial-na-ciberseguranca/. Acesso em: 25 ago. 2025.

SIQUEIRA, M. de; ANDRADE, E. J. de. ***Deepfake e privacidade****: uma análise jurídica acerca da manipulação da imagem dos usuários*. Revista Foco, v. 17, n. 8, e5679, 2024. DOI: https://doi.org/10.54751/revistafoco.v17n8-014.

VOLPI, Carlos A. **Estratégias de Mitigação de Ataques de Autenticação usando Wazuh e Inteligência Artificial:** Uma Revisão com Base no PPSI**.** *IEEE Access*, v. 4, p. 1-9, 2025. DOI: 10.1109/ACCESS.2017.DOI.