Cibersegurança aliada a Inteligência Artificial (IA)

Samuel Dias Barbosa[1], Vinicio dos Santos Martins[1], Rodrigo Rocha Rezende de Oliveira[1] e Vinicius Oliveira Souza[1]

[1]Instituto Federal do Mato Grosso - Campus Pontes e Lacerda - Fronteira Oeste (IFMT)
CEP 78250.000 – Pontes e Lacerda – MT – Brasil

{samdias028,viniciossanttos7}@gmail.com,vinicius.oliveira@ifmt.edu.br,
rodrigo.oliveira@colaborador.ifmt.edu.br

Abstract*. The article explains how artificial intelligence is becoming a vital part of cybersecurity in our digital and connected world. AI brings faster responses, continuous learning, and stronger protection against threats, helping to prevent attacks that humans might miss. Yet, the same technology that strengthens security can also be misused by criminals to create more advanced scams. The comparison with Iron Man 2 highlights this duality: technology can either save or harm, depending on who controls it. In the end, the core message is that technology only makes sense when guided by human responsibility, ethics, and awareness.*

Resumo. *O artigo mostra como a inteligência artificial está se tornando essencial para a cibersegurança em um mundo digital e conectado. A IA permite respostas rápidas, aprendizado contínuo e maior proteção contra ameaças, ajudando a prevenir ataques que antes passariam despercebidos. Porém, o mesmo poder que fortalece a segurança também pode ser usado por criminosos digitais para criar golpes mais sofisticados. A analogia com Homem de Ferro 2 revela essa dualidade: a tecnologia pode salvar ou destruir, dependendo de quem a controla. A mensagem final é clara, a tecnologia só faz sentido quando guiada por responsabilidade, ética e consciência humana.*

1. Introdução

Em um mundo cada vez mais digital, proteger informações tornou-se mais do que uma medida técnica, tornou uma necessidade humana. A sociedade está constantemente conectada: fazendo compras, trabalhando, estudando e até cuidando da saúde por meio de dispositivos e plataformas online. Nesse contexto, a cibersegurança deixou de ser um assunto restrito a profissionais de Tecnologia da Informação (TI) e passou a ser uma preocupação coletiva. Ao passo que, a inteligência artificial (IA) tem transformado a maneira de lidar com problemas complexos, oferecendo soluções que aprendem, se adaptam e tomam decisões com agilidade. Quando aplicada à segurança digital, a (IA) traz consigo um enorme potencial de proteção, mas também levanta dilemas éticos e novos tipos de riscos.

A inteligência artificial (IA) tem se destacado como uma aliada promissora, capaz de fortalecer a cibersegurança por meio da automação de processos, da detecção inteligente de ameaças e da resposta rápida a incidentes. No entanto, essa mesma tecnologia também pode ser usada por cibercriminosos, criando um jogo de forças em constante transformação.

Este artigo propõe uma reflexão sobre como a inteligência artificial tem sido integrada à cibersegurança, destacando seus benefícios, seus desafios e o papel fundamental da responsabilidade humana no uso dessas tecnologias.

2.O papel da IA na cibersegurança

A inteligência artificial (IA) é uma tecnologia que permite que máquinas aprendam com dados e tomem decisões de forma autônoma, como se tivessem uma "inteligência" própria. Na segurança digital, ela age como um guardião invisível: monitora redes e sistemas o tempo todo, aprende como é o comportamento normal e, quando algo estranho acontece, como um acesso de outro país, um arquivo suspeito ou uma tentativa de invasão, ela detecta e pode agir muito rápido, muitas vezes antes que um humano perceba. Isso faz toda a diferença em tempos em que os ataques acontecem em segundos.

> A inteligência artificial e seu aprendizado vem evoluindo constantemente nos dias atuais, expandindo-se cada vez mais a capacidade de respostas em tempo real e análise. Desde algoritmos avançados para detecção de anomalias até a construção de lógicas, têm demonstrado eficiência no combate e na construção de defesas contra ameaças. Entretanto, nas profundezas do que hoje é usado para o bem, também existem suas vertentes maléficas (Gallizzi; Kalili; Casemiro; Cruz; p.3,2024)

3.Sistemas de Detecção e Prevenção de Intrusões com IA.

Usar IA na cibersegurança traz muitos benefícios. Primeiro, a velocidade de resposta: enquanto uma pessoa pode demorar minutos ou horas para perceber um ataque, a IA pode reagir em milissegundos. Segundo a capacidade de aprendizado: ela evolui com o tempo, aprendendo com cada nova tentativa de ataque. Terceiro, ela reduz a sobrecarga de trabalho dos analistas humanos, que podem focar nas decisões mais críticas. Além disso, a IA pode prever possíveis falhas antes que elas aconteçam e até detectar ameaças que nunca haviam sido vistas antes.

A detecção e prevenção de intrusões (IDS/IPS) são pilares fundamentais da cibersegurança, atuando como verdadeiros sentinelas nas redes. Um Sistema de Detecção de Intrusões (IDS) funciona como um alarme. Ele monitora o tráfego de rede e analisa atividades para identificar possíveis ameaças. Ele pode, por exemplo, notar um comportamento anormal, como um número inusitado de tentativas de login, e alertar os administradores. O IDS não impede o ataque, mas avisa sobre ele. Já o Sistema de Prevenção de Intrusões (IPS) vai um passo além: além de detectar a ameaça, ele toma uma ação imediata para bloqueá-la, como por exemplo, interromper a conexão ou bloquear o endereço de IP do atacante.

Com a IA, esses sistemas se tornam muito mais sofisticados. Os IDS/IPS tradicionais dependem de assinaturas de ameaças conhecidas, o que os torna ineficazes contra ataques novos. No entanto, quando a IA é integrada, os sistemas podem usar algoritmos de aprendizado de máquina para identificar padrões anômalos. Em vez de apenas procurar por ameaças já catalogadas, eles aprendem o que é um comportamento "normal" na rede, como o fluxo de dados entre servidores ou o horário de acesso de funcionários. Para isso, são utilizadas abordagens de Machine Learning, como redes neurais ou análise de cluster, que adicionam essa camada de profundidade técnica à detecção. Qualquer desvio desse padrão é automaticamente sinalizado como

uma anomalia, permitindo a detecção de ameaças de dia zero (aquelas que ainda não são conhecidas). A IA permite que o IDS/IPS tome decisões em tempo real, mitigando um ataque antes que ele cause danos significativos, transformando-os de meros "alarmes" em "guardiões ativos. Em resumo, ela torna a segurança mais inteligente, adaptável e escalável.

> A utilização de IA para defesa tem tido seus avanços, ferramentas como sistemas de detecção e prevenção de intrusões (IDS/IPS) aprimorados com IA são capazes de processar dados em tempo real, aprendendo com incidentes para prever e mitigar ameaças futuras. (Gallizzi; Kalili; Casemiro; Cruz; p.7,2024)

4.A Dualidade da IA:Ferramentas de Defesa e Ataque.

Mesmo quem só usa o celular para redes sociais, pagamentos ou e-mails pode ser vítima de várias ameaças. Phishing, por exemplo, é quando alguém tenta enganar você com mensagens falsas que parecem verdadeiras, como “Atualize sua conta bancária aqui". Também há malwares, que são programas maliciosos que podem roubar dados ou travar seu computador. Além disso, há golpes que usam engenharia social, tentando manipular você emocionalmente para entregar informações. Ou seja, não é preciso ser uma grande empresa para ser alvo todos estão expostos, e por isso a segurança digital é algo que precisa estar presente no nosso dia a dia.

> O crescente avanço das ferramentas de IA, o mercado ilegal, especificamente na dark web, vem explorando essas inovações para oferecer recursos para a realização de fraudes e golpes digitais. Ferramentas como o FraudGPT, por exemplo, estão sendo comercializadas com o intuito de facilitar criações de phishing, engenharia social e ataques direcionados, utilizando IA para gerar conteúdo que engana até mesmo sistemas (Gizmod, n.p., 2024).

Essa ferramenta pode criar textos de phishing altamente personalizados e contextuais, que são muito mais difíceis de serem identificados como maliciosos por um usuário comum.

5.Cibersegurança aliada a IA e o universo de Homem de Ferro 2.

No filme Homem de Ferro 2, vemos Tony Stark lidando com um grande dilema: ele criou uma tecnologia capaz de proteger o mundo, mas que também pode ser usada para causar destruição em larga escala se cair nas mãos erradas. Isso faz com que ele carregue uma responsabilidade imensa.

Essa mesma tensão aparece hoje, de forma muito real, quando falamos sobre inteligência artificial aplicada à cibersegurança. A IA tem potencial para proteger milhões de pessoas, empresas e governos de ataques digitais, monitorando sistemas, detectando ameaças e respondendo quase instantaneamente. Ela age, de certa forma, como a armadura do Homem de Ferro: inteligente, ágil e protetora.

Mas, assim como no filme, há o outro lado. A mesma IA que defende pode ser usada para atacar. Cibercriminosos têm usado IA para criar fraudes mais sofisticadas,

enganar pessoas e ultrapassar sistemas de segurança. É como se, no mundo real, o “Homem de Ferro do bem” tivesse que lutar contra versões sombrias da própria tecnologia que criou.

Além disso, o filme mostra um conflito entre Stark e o governo, que quer controlar a tecnologia. Isso levanta um ponto central: quem deve ter o controle da IA? Quem garante que ela será usada com ética, com responsabilidade, a favor das pessoas e não contra elas?

A tecnologia é incrível, sim. Mas, como o filme mostra, ela precisa vir acompanhada de humanidade, ética e responsabilidade. Porque por trás de cada máquina, de cada código, de cada decisão automatizada… ainda são os seres humanos que decidem o rumo das coisas.

6.Conclusão

Falar sobre a união entre cibersegurança e inteligência artificial é, no fundo, falar sobre o equilíbrio entre tecnologia e humanidade. A IA tem se mostrado uma aliada poderosa, capaz de proteger sistemas, antecipar ameaças e reagir com rapidez impressionante. No entanto, essa mesma força pode se voltar contra as pessoas se for usada sem responsabilidade ou ética. Por isso, pensar o futuro da segurança digital é também pensar sobre valores, escolhas e limites humanos.

Mais do que criar máquinas inteligentes, o desafio agora é garantir que elas ajam com propósito e dentro de princípios que respeitem a sociedade. Futuras pesquisas podem contribuir muito nesse sentido, desenvolvendo mecanismos que tornem as decisões da IA mais transparentes. A "IA explicável", por exemplo, não serve apenas para gerar confiança, mas também se mostra como uma ferramenta essencial para auditar e identificar mais facilmente quando a IA está sendo usada para fins nefastos, reduzindo os riscos de uso indevido e fortalecendo a confiança entre pessoas e tecnologia. Futuras pesquisas podem contribuir muito nesse sentido desenvolvendo mecanismos que tornem as decisões da IA mais transparentes, reduzam riscos de uso indevido e fortaleçam a confiança entre pessoas e tecnologia. Além disso, é essencial que governos, empresas e universidades trabalhem juntos para formar profissionais conscientes sobre os impactos éticos e sociais da inteligência artificial.

No fim das contas, a verdadeira segurança digital não depende apenas de códigos ou algoritmos, mas da responsabilidade de quem os cria e controla. Cabe à humanidade decidir se a IA continuará sendo uma ferramenta para proteger ou uma arma para ferir. E essa escolha deve sempre ser guiada por ética, empatia e responsabilidade.

7.Referências

Cruz, J. V. D. S., Casemiro, J. V., Gallizzi, J. E. S., & Kalili, R. M. (2024). Inteligência artificial e cibersegurança: análise de ameaças emergentes e estratégias defensivas. REVISTA DELOS, 17(61), e2954. https://doi.org/10.55905/rdelosv17.n61-193. Acesso 28 abr. 2025

GIZMODO. Hackers criam FraudGPT com IA maliciosa para gerar golpes com um clique. Gizmodo Brasil, 2024. Disponível em: https://gizmodo.uol.com.br/hackers-criam-fraudgpt-com-ia-maliciosa-para-gerar-golpes-com-um-clique/. Acesso em: 10 jun. 2025

Iron Man 2. Dir. Jon Favreau. Marvel Studios, Paramount Pictures, 2010. Filme. Acesso em 12 Jun. 2025

Salem, AH, Azzam, SM, Emam, OE et al. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big Data, v. 11, art. 105, 04 ago. 2024. Disponível em: journalofbigdata.springeropen.com. Accesso em 20 Jun 2025

Mia Cate. AI Powered Intrusion Detection Systems: Challenges and Opportunities. 2025. Trabalho apresentado em janeiro de 2025. Disponível em: researchgate.net. Acesso 20 jun. 2025

Esfera Digital. FraudGPT: cibercriminosos exploram a popularidade da IA para criar ferramenta criminosa. 7 mar. 2024 esferadt.com.br. Acesso em 20 jun. 2025