ANÁLISE DO AVANÇO ACELERADO DOS MODELOS DE INTELIGÊNCIA ARTIFICIAL E SEUS IMPACTOS NO CAMPO DA CIBERSEGURANÇA

Miguel Soares Finamor

Resumo

Este trabalho desenvolve as interações entre cibersegurança e inteligência artificial, tendo como foco a aplicação da IA na área cibernética, nas questões de proteção do ambiente digital contra ciberataques, mas também discutindo o uso dos modelos inteligentes em ataques cibernéticos, aumentando a dificuldade de defesa da cibersegurança, exigindo ter conhecimentos sobre IA dos dois lados. A pesquisa evidencia avanços da IA no campo da cibersegurança, dando atenção a técnicas que os criminosos usam para o aprendizado das máquinas para realizarem o determinado crime virtual, de maneira efetiva e com resultados a curto prazo. Já na área da segurança digital, os desenvolvedores treinam as inteligências artificiais de uma forma em que elas conseguem detectar os ataques em tempo real, e assim outros modelos de IA realizam a defesa, prevenindo qualquer desvio da segurança. Ao abordar fontes e estudos relevantes, o artigo busca uma análise crítica e detalhada do potencial da inteligência artificial no fortalecimento da cibersegurança, destacando tanto suas vantagens quanto suas desvantagens.

Palavras-chave: Inteligência Artificial. Cibersegurança. Ataques Cibernéticos. Phishing.

Introdução

Nos últimos anos, houve um avanço rápido da inteligência artificial que mudou muitas áreas, como a administração, gerencia de folhas de pagamento, entre outras. Trazendo maior eficiência nos serviços. Entretanto, esse crescimento tecnológico também trouxe problemas para a sociedade, principalmente no campo da cibersegurança, que “tem como objetivo entender a forma como ataques funcionam e gerar medidas de resposta para os mesmos, garantindo a confidencialidade, integridade e disponibilidade de informações.” (BOECHAT, 2022). O uso de IA em atividades criminosas deixa fácil o acesso a informações sofisticadas por pessoas que não possuem conhecimento técnico avançado especializado no campo da segurança

cibernética. Isso abre brechas para ataques automatizados montados pelos criminosos, que utilizam a IA para administrar a automatização, e a manipulação de modelos inteligentes, que podem ser usados para achar possíveis falhas e partes vulneráveis da segurança digital. “Um ataque cibernético é geralmente uma tentativa maliciosa e coordenada por um indivíduo ou organização, com intenções maliciosas, para violar outro indivíduo ou sistema de informação da organização com o intuito de obter acesso e/ou dados do mesmo ou de terceiros.” (BOECHAT, 2022). Entretanto, assim como a IA pode ser usada para cometer crimes cibernéticos, ela também tem a capacidade de ser usada para avanços futuros e melhorias na cibersegurança. Nessa situação, se-discute: como o rápido avanço dos modelos de inteligência artificial afetam diretamente o mundo da cibersegurança, tanto nas suas fraquezas e brechas quanto nas possibilidades de proteger esse ambiente virtual? Este artigo tem como objetivo analisar de que maneira o avanço acelerado das inteligências artificiais impactam no campo da cibersegurança. Manifestando as dificuldades de grandes desafios e formas utilizadas para proteger dados digitais.

Referencial Teórico

O crescente poder da Inteligência Artificial traz evoluções notáveis, demonstrando um avanço no poder de inteligência conforme novas tecnologias vão surgindo. Um exemplo dessa capacidade de inteligência de um sistema de IA, é a criação do AlphaGO, um sistema criado em 2016 por uma equipe de laboratório de inteligência artificial do Google, o DeepMind. Esse sistema foi treinado para jogar um jogo chinês de tabuleiro chamado Go, e para testar sua capacidade, o melhor jogador do mundo de Go, foi selecionado para jogar uma partida contra essa IA, o resultado foi a vitória da máquina. Esse fato abre muitas reflexões, visto que um computador ganhou do melhor jogador do mundo de 5 a 0, evidenciando o forte poder de lógica e estratégia dessa tecnologia. Com os recentes avanços nos sistemas de IA, a comunidade de segurança cibernética utiliza modelos inteligentes (IA) para prevenir ataques, tornando-se este campo mais fortalecido. “Um exemplo interessante é a empresa britânica Darktrace, que desenvolveu um algoritmo conhecido como "Enterprise Immune System" Ela afirma que essa ferramenta detectou um ataque de ransomware. Nesta situação particular, um funcionário visitou seu E-mail pessoal da rede corporativa, permitindo a entrada de malware, esse conectou-se à rede e começou a acessar o compartilhamento SMB e criptografá-lo. Em apenas 9 segundos a

ferramenta sinalizou como uma ameaça, e 24 segundos depois tomou sozinha a decisão de interromper as atividades de gravações anormais, neutralizando o ataque e limitando o dano a uma pequena quantidade de dados.” (VEIGA, 2018). Portanto, esse avanço é fundamental para a cibersegurança, uma vez que ela também pode ser usada pelo lado adversário. “A IA adversária é o termo usado para quando o Hacker utiliza a inteligência artificial para fins maliciosos, no desenvolvimento inicial da IA o aprendizado de máquinas tem um desenvolvimento vital no tratamento de ameaças cibernéticas, porém seus algoritmos funcionam de acordo com os recursos específicos predefinidos o que significa que os recursos não predefinidos escaparão da detecção e não poderão ser descobertos. Embora a IA tenha uma capacidade exorbitante de processar informações, ela é programada por humanos o que significa que contém brechas” (LAZIC, 2019).

“Para se proteger contra os crimes cibernéticos você deve em primeiro lugar, saber quais os tipos de crime que existem. A Internet é uma infraestrutura complexa, na qual os cibercriminosos criam cerca de 57 mil sites de scam a cada semana. Em 2008, havia cerca de 10 milhões de vítimas de roubo de identidade, somente nos Estados Unidos, de acordo com um relatório da agence France Press. Os facilmente evitáveis crimes informáticos, atacam os usuários de computador através de vários métodos, tais como o uso de perseguição cibernética, assédio, invasão de privacidade, phishing e até mesmo sendo impostores online.” (SILVA; LIMA, 2018). Nota-se que, o uso de IA em golpes online é bastante recorrente no setor de comunicação digital, como e-mails, mensagens por telefone, vídeos online nas redes sociais, entre outros.

De acordo com o site do Diário do Comércio (2024), “Segundo a delegada titular da 2ª Delegacia Especializada em Crimes Cibernéticos de Belo Horizonte, Marcelle Bacellar, em 2024 já houve casos envolvendo a nova tecnologia. Ela cita como exemplo a ocorrência de um deputado que procurou a polícia após ser vítima da circulação de um vídeo em que criminosos usaram IA para simular sua voz e imagem pedindo doação para uma falsa campanha. “A IA é um campo fértil para a atuação dos golpistas”, afirma a delegada.

Esse tipo de prática é conhecido como deepfake e utiliza inteligência artificial, mais especificamente algoritmos de aprendizado profundo, para criar ou manipular conteúdo visuais e auditivos de forma extremamente realista. Isso inclui vídeos, imagens ou áudios em que a aparência, voz ou comportamento de uma pessoa é falsificado de maneira convincente.”

Metodologia

O tipo de pesquisa usado neste trabalho foi a qualitativa e quantitativa, que busca entender e discutir as consequências do avanço acelerado dos modelos de inteligência artificial no campo da cibersegurança. A pesquisa é da forma exploratória e descritiva, a fim de descobrir os principais desafios e possibilidades do uso da IA na segurança digital e nas partes vulneráveis dos sistemas digitais.

Para a criação do artigo, foi feita pesquisas bibliográficas em fontes acadêmicas e científicas, como o uso de artigos pesquisados no Google Acadêmico, pesquisas de publicações e sites profissionais e confiáveis. A coleta de dados foi a busca de estudos recentes que abordam o tema de cibersegurança com o uso de inteligência artificial, provando a atualização e a validade das informações apresentadas.

O critério de seleção da amostra incluiu a credibilidade dos autores e a pertinência dos conteúdos propostos. Priorizando publicações com revisão por pares, ou seja, materiais disponibilizados em plataformas reconhecidas na área de cibersegurança e tecnologia.

As técnicas de análise de dados coletados foram analisadas de modo interpretativo, como forma de entender as relações de IA com cibersegurança. A análise buscou achar padrões e desafios apresentados na literatura, tendo uma visão crítica e fundamentada.

Resultados

Nesta seção, será apresentado os resultados obtidos por meio da análise dos dados coletados, com informações das pesquisas bibliográficas realizadas durante o preparo do artigo.

Figura 1 - Crimes Cibernéticos mais comuns

FONTE: Martha Gabriel, 2021

De acordo com a figura acima, observa-se como o golpe de phishing é o mais realizado pelos cibercriminosos, pois é o mais fácil de ser feito e mais difícil da vítima se proteger. Segundo o site Sicredi (2025), “Phishing é um tipo de ataque cibernético que utiliza e-mails, redes sociais, mensagens de texto e ligações fraudulentas para enganar indivíduos ou empresas. O objetivo é induzir as vítimas a fornecer informações sigilosas, como senhas e dados bancários, ao se passarem por entidades confiáveis, como instituições financeiras e empresas de telefonia, por exemplo.

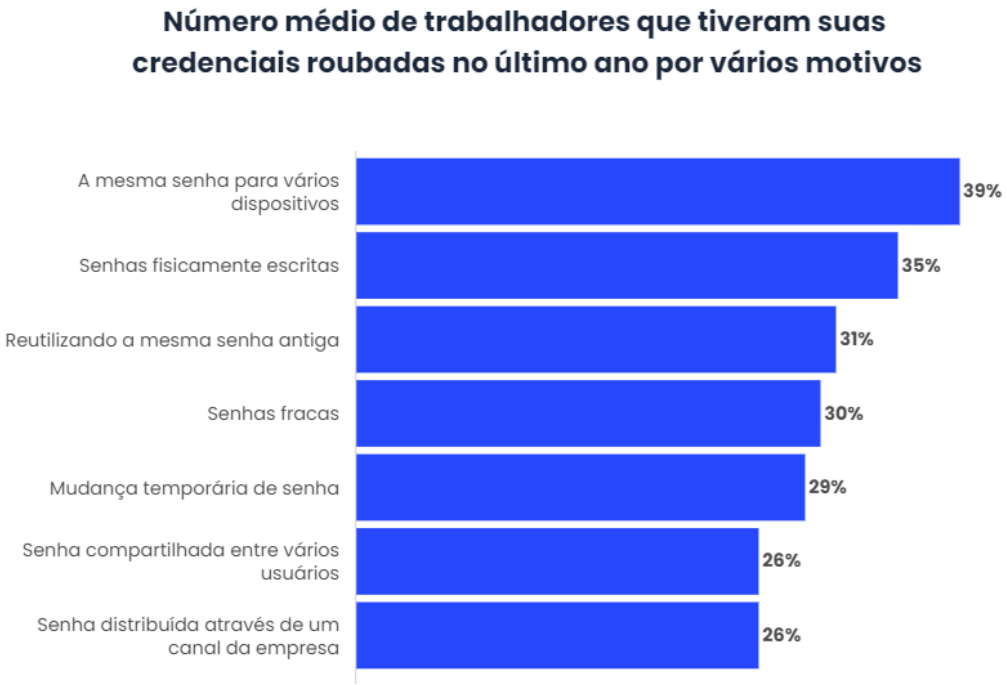
Diferentemente de outros ataques, em que os alvos são as redes, os servidores e os aplicativos instalados, no phishing outro recurso valioso é utilizado: a engenharia social. Ela consiste na manipulação psicológica de pessoas para a execução de uma determinada ação para a aquisição de informações confidenciais. Um bom exemplo de phishing é quando uma pessoa recebe um e-mail de uma instituição financeira

solicitando a confirmação de dados pessoais ou quando uma fatura de um serviço é cobrada sem a sua contratação. Ao utilizar gatilhos de emergência, um phishing bem-sucedido pode trazer inúmeras complicações.”

Mas isso é devido ao uso de IA, porque “um dos desafios que os atacantes enfrentam hoje, especialmente o phishing, é que eles realmente necessitam entender o sistema que estão atacando ou seu alvo individual, que é uma atividade que leva muito tempo. Nesse caso, ataques automatizados com o uso da IA, personalizados e inteligentes podem ser mais eficazes e rápidos, porque cada objetivo leva muito menos tempo.” (Soprana, 2017). Resumindo, o golpe fica mais simples e rápido de ser feito por causa da IA.

De acordo com o site Aiqon, “Apenas 9% das organizações afirmam nunca ter sido atacadas por phishing. 10% dizem que tiveram de lidar com 1 a 10 ataques em um ano. 37% sofreram até 50 ataques de phishing, 28% de 50 a 100 ataques e 12% mais de 100 em um período de doze meses.” (s.d.).

Figura 2- Setores empresariais que usam IA para se protegerem de possíveis ataques cibernéticos



FONTE: SOFTTEK, 2019

De acordo com a figura 2, nota-se que a parte mais investida é a de telecomunicações, provando a fraqueza da cibersegurança com os avanços da IA na questão da manipulação de textos e interações sociais.

Figura 3 - Brasil: ciberataques aumentam 38% no primeiro trimestre de 2024

FONTE: DATA CENTERDYNAMICS, 2024

Essa figura 3 apresenta a média global de ataques cibernéticos semanais por organização. Isso é um sinal alarmante, mostrando que os ataques só tendem a aumentar, é necessário um investimento de longa escala para lidar com o cibercrime, pois aumentou a porcentagem da quantidade de ataques cibernéticos desde 2021 até 2024.

Discussão

Os resultados mostram que o progresso da inteligência artificial tem um efeito grande na parte de segurança cibernética, tanto nas falhas quanto nas maneiras de se defender. Percebe-se que o emprego de IA por criminosos para fazer golpes de phishing e ataques automatizados é uma ameaça se expandindo, conforme diz Soprana (2017), que fala da eficiência dos ataques personalizados e automatizados pela utilização da tecnologia.

Além disso, os dados do site Aiqon (s.d.) mostram que os ataques de phishing ainda são um problema grande para as empresas, evidenciando como é difícil evitar eles mesmo com a melhoria da segurança. A ação do método da Darktrace, segundo Veiga (2018), ilustra bem como a inteligência artificial também pode ser uma ajuda importante na luta contra ciberataques, como nos exemplos do ransomware interrompido em poucos segundos, o que mostra o valor da tecnologia para melhorar a proteção online.

Mas além da importância dos descobrimentos, é necessário pensar em algumas limitações neste trabalho. O estudo usa principalmente fontes diretas, como textos acadêmicos e sites focados. Além disso, a rápida evolução tecnológica pode acontecer de alguns pontos discutidos se tornarem obsoletos, demandando atualizações frequentes.

Para pesquisas futuras, uma melhor forma de abordar pesquisas, seria realizando entrevistas com especialistas ou estudos de casos práticos, com o intuito de aprofundar o conhecimento dos desafios e soluções no campo da cibersegurança. Assim, aprimorando as estratégias de prevenção de ataques e ameaças cibernéticas, principalmente com a aplicação da IA.

Conclusão

Neste contexto, conclui-se que o avanço da inteligência artificial tem um efeito grande no campo da segurança online, tanto nas falhas quanto nas chances de proteção. O uso da IA pelos adversários para fazer ataques automáticos e criar golpes mostra o quão sério é o estudo dos desafios que as organizações e usuários têm no mundo digital. Mas ao mesmo tempo, usar tecnologias inteligentes na defesa e na luta contra esses perigos mostrou uma grande eficiência para diminuir riscos e reforçar a proteção dos dados.

É essencial, porém, que a comunidade acadêmica e os trabalhadores da área sigam investindo em estudos e novas tecnologias que vão com os rápidos desenvolvimentos digitais, garantindo soluções mais efetivas e melhores formas de defesa. Só com um esforço contínuo vai ser possível ajustar o poder que muda inteligência artificial com as necessidades de uma cibersegurança eficiente e cheia de adaptação às novas realidades tecnológicas

Referências

BOECHAT, Gabriel Verleun. Análise da aplicação da inteligência artificial no atual cenário de cibersegurança. 2022. Disponível em: https://diariodocomercio.com.br/economia/inteligencia-artificial-campo-fertil-para-crimes-ciberneticos/. Acesso em: 14 mar. 2025.

SANTOS, Asenate Maria; NEVES, Joao Emmanuel D. Alkmin. Exploração maliciosa do ChatGPT para ataques cibernéticos. In: FatecSeg-Congresso De Segurança Da Informação, 2023.

DOS ANJOS SILVA, Jefferson David; DE OLIVEIRA LIMA, Maria Vitória Ribas. Os principais cibercrimes praticados no Brasil. 2018.

DE ALMEIDA SOUZA, Jaqueline Patrícia; DE MORAES, Maria José. Fortalezas e fragilidades no uso da Inteligência Artificial na Cibersegurança. Revista Tecnológica da Fatec de Americana, v. 9, n. 02, p. 25-40, 2021.

GOOGLE. Computador Google vence campeão de Go. 2015. Disponível em: https://tecnoblog.net/noticias/computador-google-vence-campeao-go/. Acesso em: 14 mar. 2025.

CNN BRASIL. Ataques hackers aumentam 88% no Brasil e país segue como 2º mais atacado do mundo. 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/ataques-hackers-aumentam-88-no-brasil-e-pais-segue-como-2o-mais-atacado-do-mundo/. Acesso em: 13 mar. 2025.

MICROSOFT. O que é Inteligência Artificial para Cibersegurança?. 2025. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-ai-for-cybersecurity. Acesso em: 14 mar. 2025.

DIÁRIO DO COMÉRCIO. Inteligência Artificial: campo fértil para crimes cibernéticos. 2024. Disponível em: https://diariodocomercio.com.br/economia/inteligencia-artificial-campo-fertil-para-crimes-ciberneticos/. Acesso em: 14 mar. 2025.

FUTURO DOS NEGÓCIOS. Crimes cibernéticos mais comuns. 2024. Disponível em: https://futurodosnegocios.com.br/blog/crimes-ciberneticos-mais-comuns. Acesso em: 14 mar. 2025.

SOFTTEK. IA e modelo Zero Trust para melhorar a segurança cibernética corporativa. 2024. Disponível em: https://blog.softtek.com/pt/ia-e-modelo-zero-trust-para-melhorar-a-seguranca-cibernetica-corporativa. Acesso em: 14 mar. 2025.

DATACENTER DYNAMICS. Brasil: ciberataques aumentam 38% no primeiro trimestre de 2024. 2024. Disponível em: https://www.datacenterdynamics.com/br/not%C3%ADcias/brasil-ciberataques-aumentam-38-no-primeiro-trimestre-de-2024/. Acesso em: 14 mar. 2025.