FORTALEZAS E FRAGILIDADES NO USO DA INTELIGÊNCIA ARTIFICIAL NA CIBERSEGURANÇA

Jaqueline Patrícia de Almeida Souza[1]
Maria José Morais[2]

DOI: 10.47283/244670492021090225

Resumo
Este artigo desenvolve uma análise do uso da Inteligência Artificial na cibersegurança e tenta explorar suas fragilidades, e como ela pode ser usada para ciberataques. A Inteligência Artificial iniciou na década de 50 e ao longo dos anos vários pesquisadores contribuíram para o seu aprimoramento, técnicas como a Rede Neural proposta pelo neuropsicólogo McCulloch e o lógico Pitts , a criação de sistemas especialistas tiveram relevância em sua construção, hoje a Inteligência artificial está super avançada e abrange uma variedade de subcampos , entre as áreas que mais se beneficiaram do seu uso está a Cibersegurança aonde ela é aplicada na detecção de fraudes, investigação forense , ataques de negação (DDoS), detecção de vírus entre outros. Devido a sua capacidade de reutilizar padrões de ameaças ela pode reduzir tempo e custos. Essa capacidade tecnológica que a Inteligência Artificial traz também pode ser usada para Ciberataques , o Trojan Emotet é um exemplo de um protótipo de ataque desse tipo. Em 2017 o ataque do WannaCry que atingiu 150 países, nos deu uma amostra do que um ataque cibernético em grande escala pode promover. Por isso que especialistas temem o uso da Inteligência Artificial adversária, que tornou os ataques cada vez mais sofisticados e imprevisíveis. A inteligência artificial continuará impactando o cenário de segurança tecnológica e há muitos mais ganhos do que perda com o seu uso, e sem ela na cibersegurança não será possível inibir ataques de cibercriminosos.
Palavras Chaves: Inteligência Artificial. Cibersegurança. Ciberataque

Abstract
This article develops an analysis of the use of artificial intelligence in cybersecurity and tries to explore its weaknesses, and how it can be used for cyber-attacks. Artificial Intelligence began in the 1950s and over the years several researchers have contributed to its improvement, techniques such as the Neural Network proposed by neuropsychologist Mcculloch and the logician Pitts , the creation of expert systems had relevance in its construction, today the artificial intelligence is super advanced and covers a variety of subfields , among the areas that benefited most from its use is the cybersecurity where it is applied in the detection of fraud, forensic investigation, denial attacks (Ddos), virus detection, and more. Because of its ability to reuse threat patterns it can reduce time and costs. This technological capability that Artificial Intelligence brings can also be used for Cyberattacks, the Trojan Emotet is an example of a prototype attack of this type. In 2017 the Wannacry attack that hit 150 countries gave us a taste of what a large-scale cyber-attack can do. This is why experts fear the use of opposing Artificial Intelligence, which has made attacks increasingly sophisticated and unpredictable. Artificial intelligence will continue to impact the technological security landscape and there are many more gains than losses from its use, and without it in cybersecurity it will not be possible to inhibit cyber-criminal attacks.

[1] Tecnóloga em Segurança da Informação pela Fatec Americana. E-mail: jaqueline.souza17@fatec.sp.gov.br
[2] Tecnóloga em Segurança da Informação pela Fatec Americana. E-mail: mariajdemorars@hotmail.com

Keywords: *Artificial Intelligence. Cybersecurity. Cyberattack*

Introdução

A inteligência artificial (IA) tem evoluído muito e está presente em todas as áreas, entre elas na cibersegurança. Na cibersegurança várias empresas vêm investindo muito dinheiro e tempo usando a Inteligência artificial como uma ferramenta de defesa a ataques cibernéticos. Porém vemos que a Inteligência artificial também tem potencial para ser usada para ataques cibernéticos de grande escala criando mais possibilidades para os cibercriminosos.

Especialistas na área de segurança da informação alertam que estamos em uma pandemia de Ciberataques e o ano de 2021 pode causar 6 trilhões de prejuízos financeiros em todo o mundo (DA REDAÇÃO,2021).

Empresas estão investido muito dinheiro na área da inteligência Artificial, e a área de segurança cibernética deve crescer cerca de 12,5% em 5 anos estima-se em até 2027 o mercado irá movimentar US$403 bilhões (DA REDAÇÂO,2021).

A evolução da inteligência artificial é inevitável e a sua aplicação na cibersegurança é fundamental uma vez que ela também pode ser usada pelo lado adversário.

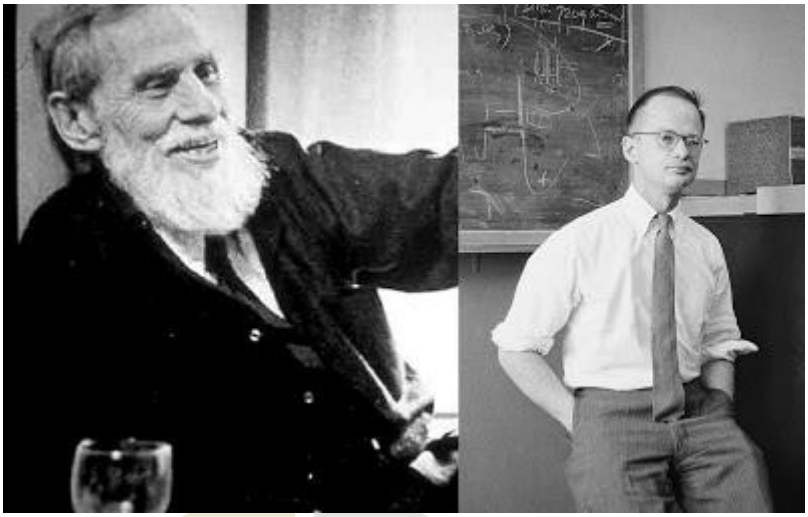
Assim, o objetivo principal desse artigo é demostrar os pontos fortes e fracos do uso da IA na cibersegurança, mostrando que ela contribuiu globalmente para melhorar a segurança das empresas, mas também contribuiu para criar ameaças. Inicialmente é abordada a história e a evolução da Inteligência artificial dando ênfase nos estudos de aplicações baseadas para parte de segurança. Em seguida é apresentada a definição de cibersegurança e trançamos a aplicação da IA nela com alguns estudos de casos de empresas que investiram em IA.

1 Inteligencia Artificial

A Inteligência Artificial (IA) é uma das ciências mais recentes. Historiadores atribuem a primeira referência a inteligência artificial ao matemático Alan Turin que em 1950 escreveu o artigo "Computing Machinery and Intelligence" (KAUFMAN, 2018), e atualmente pode estar relacionada a qualquer campo, desde áreas de uso geral, como aprendizado ao uso em tarefas específicas como jogos de xadrez, diagnóstico de doenças, sendo potencialmente relevante já que sistematiza e automatiza tarefas intelectual. (GOMES , 2010)

O nome inteligência artificial surgiu na década de 50, para ser mais exato em 1956, em uma conferência de verão na Faculdade de Dartmouth em New Hampshire nos Estados Unidos. (KAUFMAN, 2018). Em 1943, o neuropsicólogo McCulloch e o lógico Pitts que aparecem na figura 1 propuseram o primeiro modelo matemático para um neurônio, Modelo de Neurônio de McCulloch e Pitts (modelo MCP). (MADSEN; ADAMATTI, 2011).

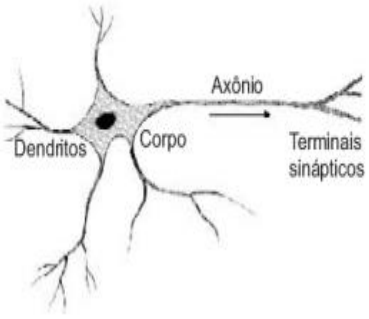
Figura 1-Warren McCulloch e Walter Pitts



Fonte: JJ, 2017.

Este modelo se baseia em uma simplificação do neurônio biológico conforme demonstrado na figura 2.

Figura 2- Representação simplificada de um neurônio humano



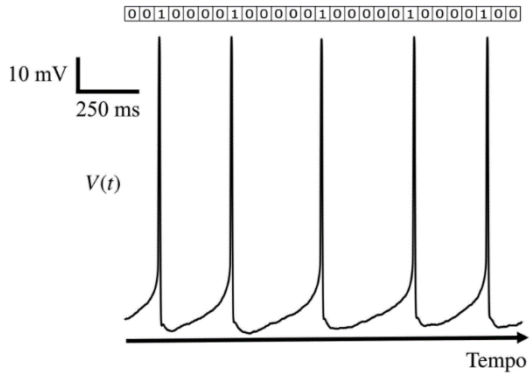
Fonte: FERNEDA, 2006.

Os dendritos captam os sinais recebidos e os envia ao corpo do neurônio aonde esses são processados. Depois, o corpo envia um novo impulso pelo axônio que transmite aos neurônios vizinhos. (RODRIGUES, 2018)

> "As interligações entre os neurônios ocorrem através das sinapses, pontos de contatos entre os axônios e os detritos de dois neurônios distintos as quais convertem os impulsos elétricos e reações químicas utilizando substâncias químicas conhecidas como neurotransmissores" (MADSEN; ADAMATTI, 2011, p. 16).

A atividade de um neurônio é binária. O neurônio dispara (atividade = 1), ou não dispara (atividade = 0), conforme a figura 3;

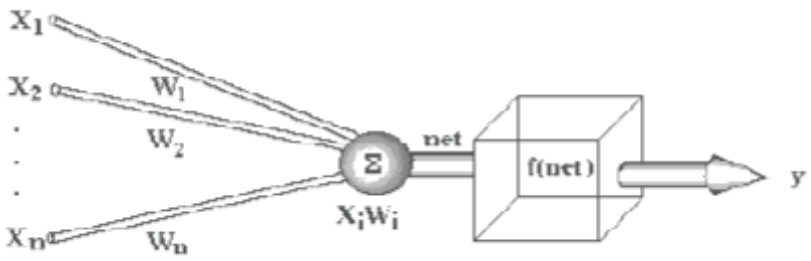
Figura 3- Registro eletrofisiológico in vitro de uma célula piramidal do hipocampo do rato



Fonte: CORDEIRO, 2019.

A rede neural umas das técnicas utilizadas em IA é constituída por linhas direcionadas, sem pesos, ligando os neurônios. Essas linhas (inspiradas nas sinapses) podem ser excitatórias ou inibitórias (positivas ou negativas);

Figura 4 - Neurônio artificial no modelo MCP



Fonte: MADSEN; ADAMATTI, 2011

Conforme a figura 4, cada neurônio artificial é composto por um vetor de entradas X = [x1, x2,...xn] que correspondem aos dendritos do modelo biológico. Em cada entrada temos um peso Wi, que define o grau de conexão entre os dois neurônios. Tendo um valor positivo, ele age como um excitador e, caso contrário, ele inibe a conexão. Se o valor for zero, não existe a conexão. (MADSEN; ADAMATTI, 2011).

Em 1958, John McCarthy definiu a linguagem de programação LISP (List Processing) que se transformou na linguagem dominante da IA e publicou um artigo intitulado "Program With common sense". (BARANAUSKAS,1993). Em 1959, a IBM produz alguns dos primeiros programas de IA como *Geometry Theorem* prover (KAUFMAN, 2018).

Na década de 1970 surgiu um sistema conhecido como MYCIN que foi desenvolvido na Universidade de Stanford para a seleção de antibióticos em pacientes com infecção severa. O programa foi amplamente testado e apresentou desempenho semelhante ao de especialistas na

área de doenças infecciosas (BARANAUSKAS,1993) embora o programa nunca tenha sido usado na prática e tenha desempenho aceitável em aproximadamente 69% dos casos (YU *et al*, 1979).

Em 2016, a companhia ingressa *DeepMind* criou um sistema de IA chamado AlphaGO, desenvolvido para jogar um jogo asiático chamado de Go, que é considerado mais complexo que uma partida de xadrez e o sistema venceu o melhor jogador do mundo.

O processo usado para esse jogo denominado *Deep learning* (aprendizado profundo) e o mesmo usado pelo Facebook para carregar o feed ou pelo Google para trazer as respostas ou anúncios de acordo com o perfil do usuário, Amazon e Netflx recomendam filmes e livros usando a mesma tecnologia (KAUFMAN, 2018)

Existe tanta informação e conteúdo sobre a inteligência artificial que é muito difícil achar uma definição formal, assim usaremos algumas definições de pesquisadores de IA. "Uma máquina é inteligente se ela é capaz de solucionar uma classe de problemas que requerem inteligência para serem solucionados por seres humanos'' (MCCARTHY; HAYES, 1969, p.19).

Assim, a "Inteligência Artificial é a parte da ciência da computação que compreende o projeto de sistemas computacionais que exibam características associadas, quando presentes no comportamento humano, à inteligência'' (BARR; FEIGENBAUM, 1981, p.12).

2 O uso da Inteligencia Artificial na cibersegurança

Antes de relacionar a Inteligência artificial com a Cibersegurança, vamos definir o que é cibersegurança. LU et. Al (2018, p. 112) define como:

> "A abordagem e as ações associadas aos processos de gestão de risco de segurança seguida pelas organizações e Estados para proteger a confidencialidade, integridade e disponibilidade de dados e bens utilizados no ciberespaço. O conceito inclui: orientações, políticas e recolha de salvaguardas, tecnologias, ferramentas e formação para permitir a melhor proteção para o estado do ambiente cyber e dos seus utilizadores (*apud* SCHATZ, 2017)".

Portanto o conceito de Cibersegurança existe antes da aplicação da IA nesse ambiente, porém é inquestionável que a aplicação da inteligência artificial é primordial para resolução da maioria dos casos.

A IA na cibersegurança é aplicada com sucesso na detecção de fraudes com cartão de crédito, investigação forense, ataques de negação de serviços (DDoS), detecção de vírus e Spam (KUMBHAR, 2014, p. 5893-5898).

Há inúmeros casos de uso nos quais a IA é interessante para aplicações de cibersegurança, como a busca por anomalias no padrão de comportamento de pessoas, dispositivos, dados e aplicações em escala e fazer previsões precisas de ameaças aos órgãos públicos ou empresa, sendo assim ela se torna uma ferramenta preditiva que permite que seja implementado defesas antes de um ataque específico (ANGGRAINI,OLIVER, 2019).

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).

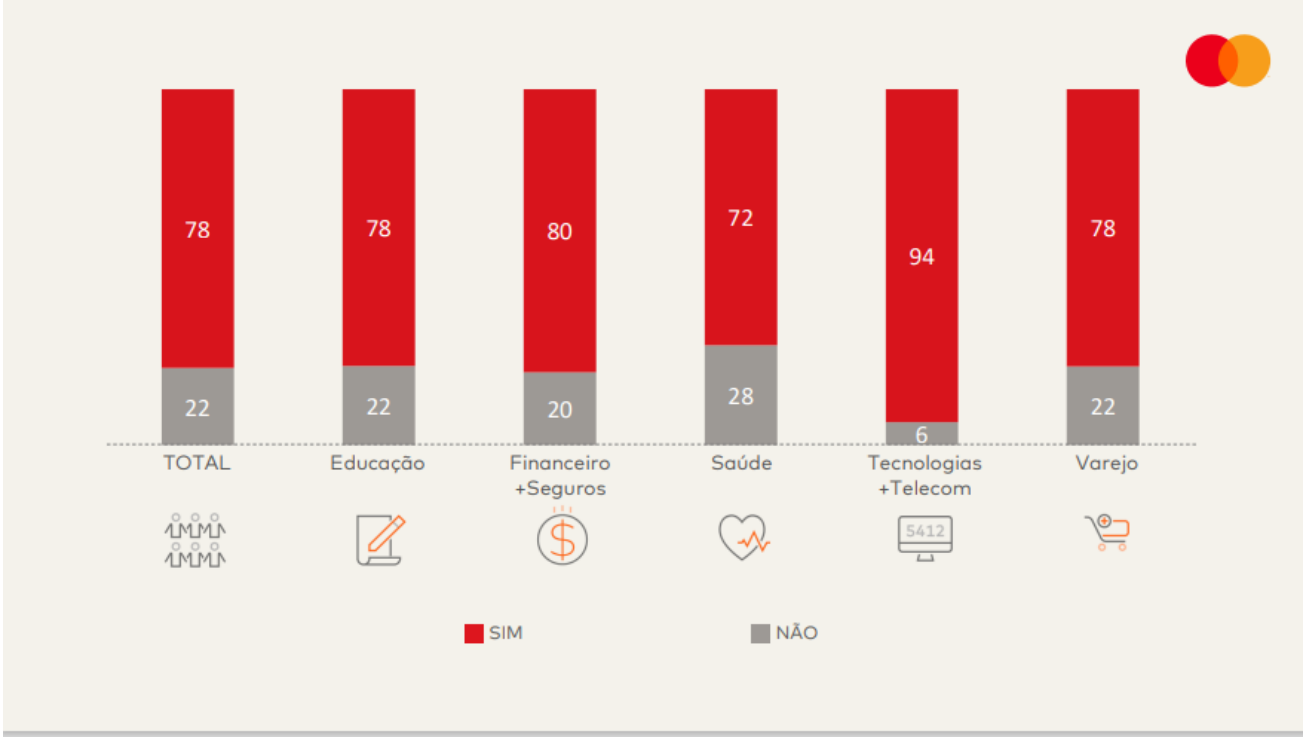
Embora a conscientização das empresas sobre as ameaças cibernéticas tenha aumentado, e muito dinheiro tenha sido investido para combater os crimes cibernéticos, a capacidade das organizações de proteger totalmente seus ativos virtuais ainda é desconhecida (WIRKUTTIS,KLEIN, 2017).

Um dos principais desafios da implementação da IA ocorre porque ela requer mais recursos financeiros do que as soluções tradicionais de segurança cibernética sem IA (LAZIC,2019).

Um estudo da Mastercard em parceria com o Datafolha, mostra que 57% das empresas brasileiras sofre ataques digitais, e dentro dessa porcentagem de empresas atacadas somente 32% possui uma área de cibersegurança. Embora uma minoria dessas companhias tenha efetivamente uma área dedica a Cibersegurança , 80% de empresas de todos os setores a considera primordial porém 39% destaca que ela não é prioridade no orçamento. A maioria das empresas apontadas na pesquisa diz ter um plano caso sofra um ataque cibernético , mas apenas um terço dela efetuou de fato teste de prevenção nos últimos 3 meses que antecederam a pesquisa. (VILELA, 2021)

Vilela (2021) destacou que a pesquisa também trouxe os dados sobre profissionais da área de cibersegurança, conforme vemos na figura 5 :

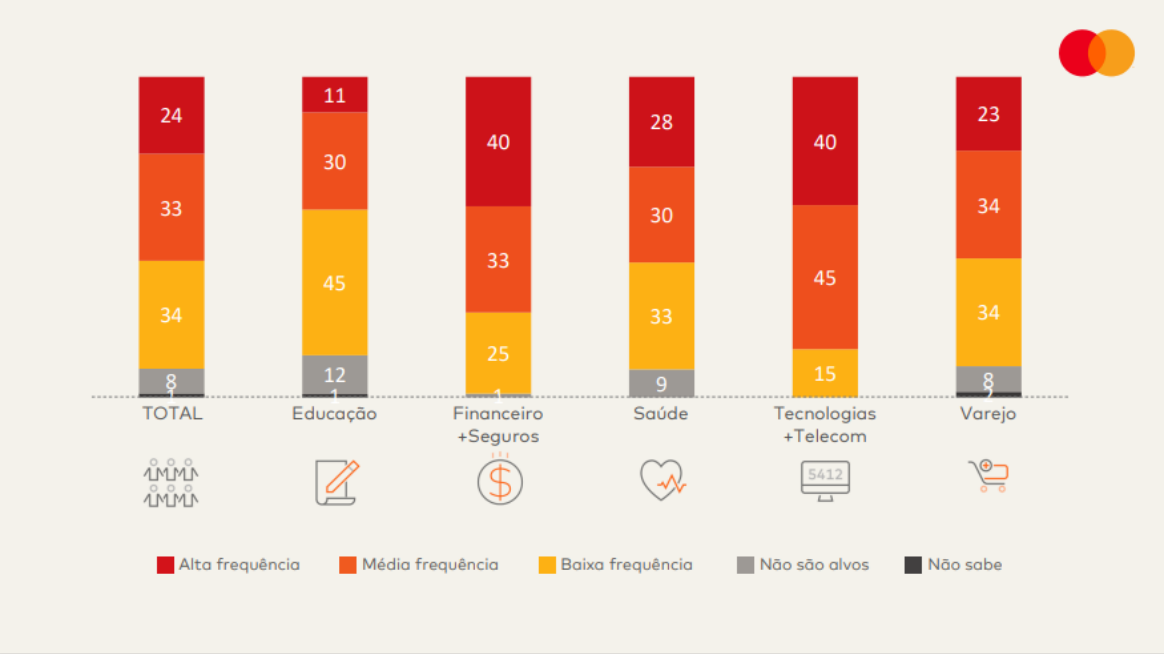
Figura 2 -Contratação de Profissionais de TI | Crédito: Mastercard



Fonte: VILELA, 2021.

A pesquisa também trouxe dados sobre os setores mais afetados conforme vemos na figura 6 , os ataques foram divididos em intensidade , e o resultado mostra que a área financeira e seguros juntamente com tecnologias e Telecom são as mais afetadas assim , como são as áreas que mais investem dinheiro em segurança (VILELA, 2021).

Figura 3-Frequência de ataques cibernéticos para cada setor de crédito: Mastercard



Fonte: VILELA, 2021

Além disso, a IA consegue reutilizar os padrões de ameaças para identificar novos Incidentes , o que reduz tempo e custos as ameaças cibernéticas são basicamente causadas por ações maliciosas que podem ocorrer por motivos econômicos, políticos ou militares (WIRKUTTIS,KLEIN,2017).

Existem dois desafios importantes e interligados em IA: segurança e privacidade. No quesito segurança incluímos o acesso ilegal a informações e, em relação a privacidade como violação da confidencialidade e dados pessoais, por exemplo (GOULART,2012).

Atualmente, 5% das tecnologias projetadas para cumprir as leis de privacidade contam com o uso de inteligência artificial. No entanto, segundo previsão da consultoria Gartner, Inc., até 2023, esse número aumentará para 40% (TECH, 2020).

O mercado de cibersegurança fatura cerca de US$ 176,5 bilhões e tem estimado um crescimento de 12,5% em 5 anos e em ate 2027 o esperado é uma movimentação de 403 bilhões (DA REDAÇÃO,2021).

3 Ciberataques x Inteligencia Artificial

Se por um lado a IA tem auxiliado na cibersegurança, ela também tem sido usada nos ataques. Os problemas de segurança são criados por pessoas mal-intencionadas com o objetivo de tirar vantagem própria (TELES,2015)

Ciberataques é a utilização de códigos maliciosos para alterar o código do computador e suas redes (JOSE,GRAÇA,2013)

Os avanços da ciência e da tecnologia de IA podem também ser aproveitados por criminosos Cibernéticos, que podem utilizar e adaptar essa tecnologia para criar softwares mal intencionados mais complexos e com um custo menor (LI,2018)

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).

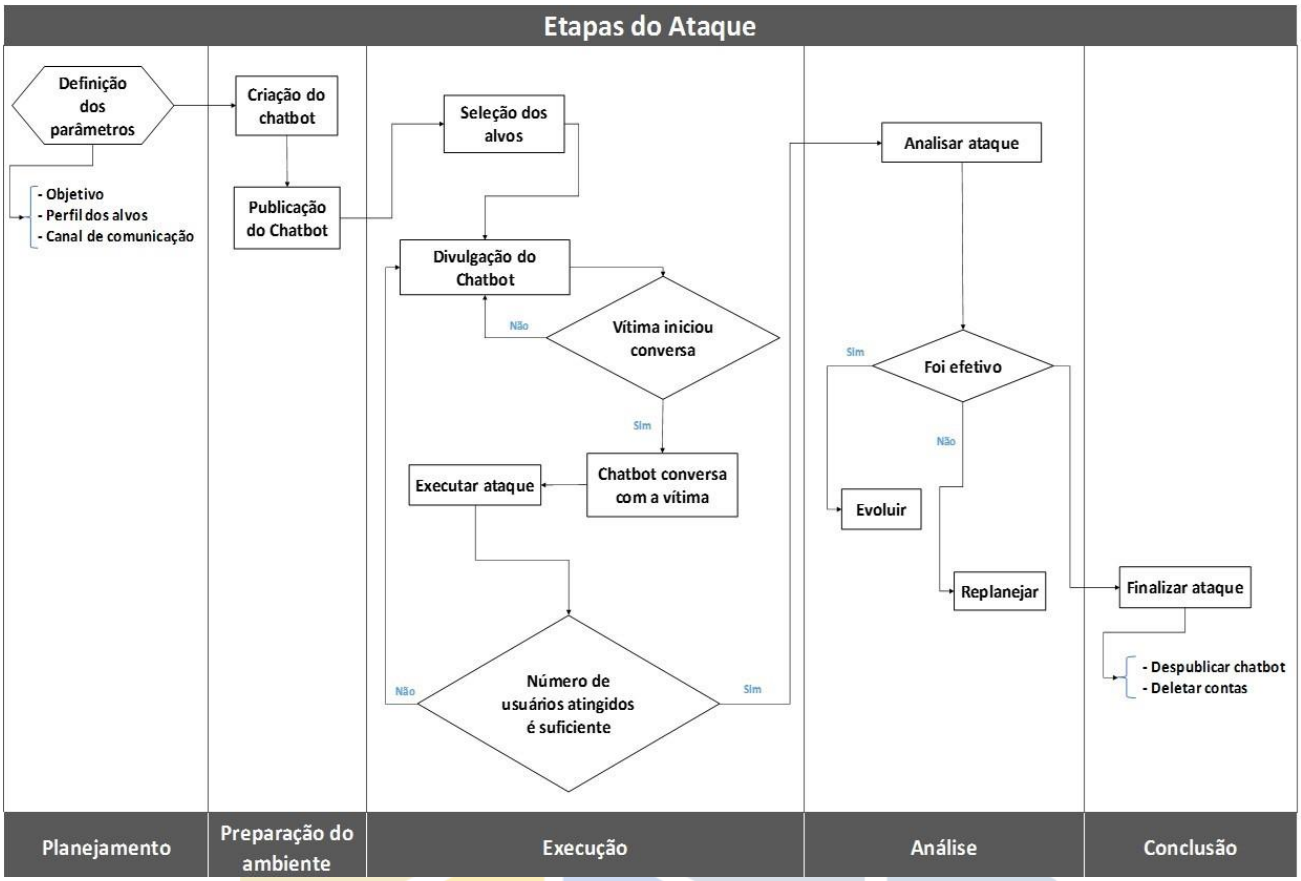
Em maio de 2017, 200.000 computadores foram invadidos pelo vírus *WannaCry* em 150 países , este ataque sem precedentes na história da Internet deixou funcionários públicos e empresários alertados sobre o futuro dos ataques cibernéticos em grande escalas (PASSARINHO, 2021).

O *Trojan* emotet é um grande exemplo de protótipo de IA, seu principal mecanismo de ataque é *spam-phishing* enviado ao e-mail da vitima , ele pode inserir-se automaticamente em tópicos de e-mail pré-existentes o que faz parecer mais autêntico e faça a vitima a clicar. (SHOAIB,2016) .

A IA reduziu o tempo, esforço e custo para os cibercriminosos, o processo de criação de *Malware* foi automatizado o resultado são ataques cibernéticos em uma escala maior, por isso as empresas de tecnologia precisam fazer parcerias com instituições acadêmicas , um exemplo é a parceria entre a empresa AVAST e a Universidade Técnica Tcheca (The Czech Technical University, CTU) na cidade de Praga. Em um estudo eles combinaram os riscos de mais de 100milhões de dispositivos. Os objetivos do laboratório incluem a publicação de pesquisas avançadas no campo e o aprimoramento do mecanismo de detecção de *malware* do Avast, incluindo seu algoritmo de detecção baseado em inteligência artificial (PECHOUCEK, 2020).

A engenharia social aplicada pelos *hackers* pode ser potencializada com o uso de *chatbots,* Nunes (2017) nos mostra que a empresa Take Blip fez um estudo de caso para mensurar o sucesso de um ataque de engenharia social usando *chatbot* . O estudo de caso seguiu as etapas conforme a figura 7

Figura 4 – Etapa do estudo de caso pela empresa Take Blip



Fonte: NUNES, 2017.

Foi criado um *chatbot* sobre vagas de emprego em uma página dentro do facebook , quando o usuário mandava uma mensagem ele passava a interagir com o *chatbot* conforme a figura 8:

Figura 5- Estudo de caso interação do usuário

Fonte: NUNES,2017.

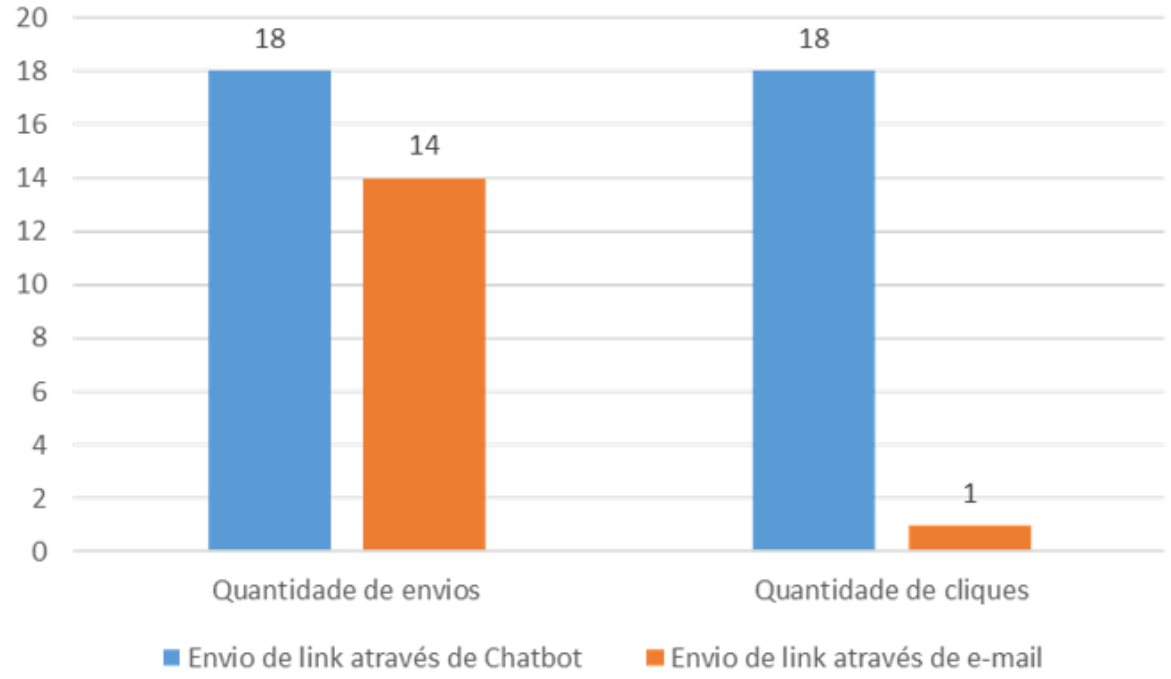
Esse teste teve duração de 12 dias, nesse período 18 pessoas conversaram com o chatbot. Um total de 100% das pessoas clicaram no 1º link que foi enviado solicitando o cadastro profissional, conforme a figura -9

Figura 6 – Estudo de Caso envio de link

Fonte: NUNES,2017.

Na pesquisa, 78% das pessoas que acessaram o link preencheram o perfil. Então foi enviado um novo link com sugestões de vagas baseado nas respostas do usuário. Nesse novo link era solicitado informações pessoais como nome , e-mail , telefone , ultima empresa que trabalhou e cargo. 71% das pessoas que tinha esse novo link preencheram essas informações. Além disso para fazer a comparação demonstrada na figura 7 foi enviado para essas pessoas um e-mail sobre as buscas de vagas com um link . Foram enviados 14 e-mails no total e somente 1 foi aberto , na figura 10 podemos observar um gráfico comparativo

Figura 7- gráfico comparativo entre chatbot x email



Fonte: NUNES,2017

Qual é a principal diferença entre um ataque cibernético humano e usando inteligência artificial? para quem sofre o ataque não há muita diferença. Em sua forma mais básica, um ataque inteligente é uma versão automatizada de um ataque liderado por humanos. 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).

DeepAttacks é a utilização de conteúdo gerado por IA ,para atacar outra IA , esse ataque é baseado em rede neural adversária, um exemplo apontando pela Avast foi o uso do algoritmo para faze-lo pensar que um sinal de Pare indicava um limite de 70KM/H (BRITO, 2019)

Pesquisas no campo da inteligência artificial (IA) mostraram que redes neurais profundas (DNNs) com bom desempenho são extremamente vulneráveis a ataques adversários. Ao adicionar alterações granulares às entradas de DNN, um invasor pode enganar o DNN para que ele emita decisões erradas. Para combater essa ameaça é necessário treinamento de oponentes, fazer suposições específicas não aplicável a testes Ataque de Injeção Falsa de Dados (FDIA), hipótese do método de detecção de adversário onde os oponentes seguem uma distribuição diferente das entradas normais, e o DNN é treinado para distinguir o exemplo do oponente Antes de encaminhá-los para o DNN funcional (LI,2021)

Especialistas em Cibersegurança acreditam que em 2021 os crimes Cibernéticos irão evoluir ,segundo eles no ultimo ano os *Hackers* tiveram a oportunidade de avaliar máquinas que eles infectaram e adquiriram mais conhecimentos do que nunca e que os *ransomware*

continuaram cada vez mais sofisticados , já que algumas companhias industrias pagam o resgate(EMM,2021)

É o caso da empresa JBS que pagou US$11 milhões a *Hackers* em maio desse ano , o CEO da JBS explicou que foi uma difícil decisão tomada após consultar diversos especialistas da área de segurança digital e que estes alertaram a respeito do risco relacionados aos dados sensíveis dos clientes (ANSA, 2021)

Outra empresa que em 2021 sofreu um ataque cibernético foi a Pipeline principal empresa de dutos de combustível dos Estados Unidos da América (EUA) a empresa pagou ao *Hacker* cerca de US$4,4 milhões (DA REDAÇÃO,2021)

Podemos ver que os ciberataques é uma ameaça de escala global , o banco suíço Julius Baer apontou em seu relatório que a economia global pode sofrer um prejuízo causado por invasões de 6 trilhões (DA REDAÇÃO,2021).

Considerações finais

A inteligência Artificial está presente em todas as áreas principalmente na área de segurança cibernética, muitas empresas vem investido muito nesse área.

O mercado de cibersegurança gera uma receita de US$176,5 bilhões , as empresas de cibersegurança estão listadas como em expansão mesmo assim não fica claro se ao longo do prazo a IA tornará a segurança cibernética mais fácil ou mais difícil.

Por um lado teremos máquinas com sistemas cada vez mais complexos baseados sua construção em IA e com a capacidade de busca por anomalias maior , pelo outro temos o uso da IA adversária, com potencial de ataque extremamente eficaz.

A habilidade essencial da IA para aprender e se adaptar trará uma nova era na qual ataques altamente personalizados e personificados por humanos são escalonáveis. O mecanismo de IA ofensivo será capaz de sofrer mutação à medida que aprende sobre seu ambiente e comprometer sistemas habilmente com chance mínima de detecção. Consequentemente, os ataques futuros seriam mais penetrantes; dando um certo grau de garantia no sentido de alcançar os objetivos desejados. Portanto, é importante analisar a IA ofensiva no domínio cibernético para uma melhor compreensão das ameaças cibernéticas habilitadas para IA.

Empresas que não implementarem soluções baseadas na inteligência artificial são as que mais sofreram consequências

Referências bibliográficas

ANGGRAINI, A. R.; OLIVER, J. Symbiotic Artificial Intelligence and Its Challenges in Cybersecurity and Malware Research. Journal of Chemical Information and Modeling, v. 53, n. 9, p. 1689–1699, 2019.

ANSA. **JBS paga US$ 11 milhões a hackers para resgatar acesso a dados**. 2021. Disponível em: https://istoe.com.br/jbs-pagou-us-11-milhoes-a-hackers-para-resgatar-acessos/. Acesso em: 03 jun. 2021.

BARANAUSKAS, M. C. C. **Procedimento, função, objeto ou lógica:** linguagens de programação vistas pelos seus paradigmas. In: VALENTE, José Armando, Org. Computadores e conhecimento: repensando a educação. Campinas, NIED/UNICAMP, 1993.

BARR, A.; Feigenbaum, E. A. **The Handbook of Artificial Intelligence**, Vol. I-II. Los Altos, California: William Kaufmann Inc. 1981.

COLUMBUS, L. **10 empresas de cibersegurança para acompanhar em 2019**. 2019. Disponível em: https://forbes.com.br/negocios/2019/06/10-empresas-de-ciberseguranca-para-acompanhar-em-2019/. Acesso em: 01 jun. 2021.

BRITO, P. **IA vem com tudo nos ataques de 2019**. 2019. Disponível em: https://www.cisoadvisor.com.br/ia-vem-com-tudo-nos-ataques-de-2019/. Acesso em: 10 jun. 2021.

CORDEIRO, V. L. *et al.* Aplicações da teoria da informação à neurociência. **Revista Brasileira de Ensino de Física**, São Paulo, v. 41, n. 2, 2019.

REDAÇÃO, Da. **Bug bounty: a solução para ciberataques que o Brasil precisa conhecer**: entender a diferença entre cibercriminoso e bughunter ajuda a reduzir a confusão em torno do termo hacker. 2021. Disponível em: Bug bounty: a solução para ciberataques que o Brasil precisa conhecer. Acesso em: 08 jun. 2021.

DA REDAÇÃO. **Setor de cibersegurança fatura US$ 176,5 bi e deve crescer 12,5% em 5 anos**: até 2027, o mercado de cibersegurança deve movimentar us$ 403 bilhões, de acordo com estudo da bmrc. Até 2027, o mercado de cibersegurança deve movimentar US$ 403 bilhões, de acordo com estudo da BMRC. 2021. Disponível em: https://www.cisoadvisor.com.br/setor-de-ciberseguranca-fatura-us-1765-bi-em-2020-e-deve-crescer-125-em-5-anos/. Acesso em: 04 jun. 2021.

DA REDAÇÃO. **Senha para VPN da Colonial Pipeline estava na dark web**: descoberta foi feita pelos peritos da mandiant, empresa especializada em forensics, contratada pela colonial para investigar o incidente. Descoberta foi feita pelos peritos da Mandiant, empresa especializada em forensics, contratada pela Colonial para investigar o incidente. 2021. Disponível em: https://www.cisoadvisor.com.br/senha-para-vpn-da-colonial-pipeline-estava-na-dark-web/. Acesso em: 10 jun. 2021.

EMM, D. **Previsões: o que 2021 tem reservado para a cibersegurança?**: especialistas em cibersegurança compartilham suas previsões sobre como os crimes cibernéticos e o cenário de ameaças devem evoluir em 2021.. Especialistas em cibersegurança compartilham suas previsões sobre como os crimes cibernéticos e o cenário de ameaças devem evoluir em 2021.. Disponível em: https://www.kaspersky.com.br/blog/secure-futures-magazine/previsoes-o-que-2021-reserva-para-a-ciberseguranca/17184/. Acesso em: 09 jun. 2021.

FERNEDA, E. Redes neurais e sua aplicação em sistemas de recuperação de informação. **Revista Ciência da Informação.** Brasília, v. 35, p. 25 – 30, jan./abr. 2006.

GOMES, D. S. Inteligência Artificial: Conceitos e Aplicações. **Revista Olhar Científico** – Faculdades Associadas de Ariquemes, Ariquemes – RO V. 01, n.2, p. 234 ago./dez. 2010.

GOULART, G. D. **Segurança da informação e a proteção contra a violação de dados pessoais: A confidencialidade no Direito do Consumidor**. 2012. 215 f. Dissertação (Mestrado) - Curso de Direito, Universidade Federal do Rio Grande do Sul, Portol Alegre, 2012.

IBM. **Inteligência artificial - IA Cyber Security para um tipo de segurança cibernética mais inteligente**. Disponível em: https://www.ibm.com/br-pt/security/artificial-intelligence. Acesso em: 10 abr. 2021.

JJ. **Psychon and MCculloch Pitts neurons.** [S.I]. Nov. 2017. Disponível em <https://infonintelli.blogspot.com/2017/11/psychon-and-mcculloch-pitts-neurons.html> Acesso em: 12 jun. 2021.

JOSÉ, P.; GRAÇA, B. **O Ciberataque como Guerra de Guerrilha O Caso dos Ataques DoS / DDoS à Estónia , Geórgia e ao Google - China**. 2013. Disponível em: <https://www.repository.utl.pt/bitstream/10400.5/8000/1/Tese.pdf>.

KAUFMAN, D. **A inteligência artificial irá suplantar a inteligência humana.** Barueri-SP: Estação Das Letras E Cores, 2018.

KUMBHAR S. R. An overview on use of artificial intelligence techniques in effective security management. **International Journal of Innovative Research in Computer and Communication Engineering,** Maharashtra - Índia, vol. 2, n. 9, p. 5893-5898, set. 2014.

LAZIC, L. Benefit From AI in Cybersecurity. **The 11th International Conference on Business Information Security**, v. 1, n. October, p. 1–8, 2019.

LI, J. H. Cyber security meets artificial intelligence: a survey. **Frontiers of Information Technology and Electronic Engineering**, v. 19, n. 12, p. 1462–1474, 2018.

LI, J.; YANG, Y.; SUN, J. S.; *et al*. **Towards Adversarial-Resilient Deep Neural Networks for False Data Injection Attack Detection in Power Grids**. p. 1–12, 2021. Disponível em: <http://arxiv.org/abs/2102.09057>.

LU et. Al. **BIM and Big Data for Construction Cost Management**. Abingdon, Oxon: Routledge, 2019. P. 112.

MADSEN, C. A. B. C. W.; ADAMATTI, D, F. NeuroFURG: uma ferramenta de apoio ao ensino de Redes Neurais Artificiais. **Revista Brasileira de Informática na Educação**, Rio Grande do Sul - RS, v. 19, ano 2011, ed. 2, p. 15-24, 24 ago. 2011. Disponível em: <https://www.br-ie.org/pub/index.php/rbie/article/view/1274/1173>. Acesso em: 5 nov. 2020.

MCCARTHY,J.; HAYES,P.J.**Some philosophical problems from the standpoint of Artificial int elligence**. Computer Science Department. Universidade de Standford. Standford, CA. 1969..

PASSARINHO, N. **Mundo vive pandemia de ciberataques e Brasil está despreparado, diz CEO de empresa que descobriu megavazamento**. 2021. Da BBC News Brasil em Londres. Disponível em: https://www.bbc.com/portuguese/brasil-56048010. Acesso em: 01 jun. 2021.

PECHOUCEK, M. **Previsões que a IA trará na próxima década**. 2020. Disponível em: http://www.mundodigital.net.br/index.php/noticias/ti/13318-previsoes-que-a-ia-trara-na-proxima-decada. Acesso em: 13 jun. 2021.

RODRIGUES, C. A. S. P. **Implementação de redes convolucionais para a segmentação de imagens em tempo real com vistas à aplicação em robôs autônomos com dispositivos de visão de baixo custo**. 2018. 110 f. Dissertação (Mestrado em engenharia elétrica e computação) - Escola de Engenharia Elétrica, Mecânica e de Computação (EMC), Universidade Federal de Goiás, Goiânia.

SHOAIB, M. AI-Enabled Cyber Weapons and Implications for Cybersecurity. **Journal of Strategic Affairs of**, p. 9–37, 2016.

SOPRANA, P. **A inteligência artificial pode ser usada em ciberataques?**: 2017. Disponível em: https://epoca.oglobo.globo.com/tecnologia/experiencias-digitais/noticia/2017/09/inteligencia-artificial-pode-ser-usada-em-ciberataques-diz-pesquisador.html. Acesso em: 01 jun. 2021.

TELES, T. M. F. P. S. T. **Deteção de outliers** Dissertação para obtenção do grau de Mestre em Ciências Militares Navais, na especialidade de Fuzileiros. 2015.

VEIGA, A. P. **Applications of Artificial Intelligence to Network Security**. n. March, 2018. Disponível em: <http://arxiv.org/abs/1803.09992>.

VILELA, L. **Só 21% das empresas têm cibersegurança como prioridade no orçamento.** Disponível em: https://www.consumidormoderno.com.br/2021/06/01/empresas-ciberseguranca-prioridade/. Acesso em: 05 jun. 2021.

WIRKUTTIS, N.; KLEIN, H. Artificial Intelligence in Cybersecurity – Current Use-Cases and Capabilities Emer. **Cyber, Intelligence, and Security**, v. 1, n. 1, p. 103–119, 2017.Disponivel em:< https://www.academia.edu/36264684/Artificial_Intelligence_in_Cybersecurity>Acesso em 10 Mai 2021

YU, V. L. et al. Antimicrobial selection by a computer: A blinded evaluation by infectious diseases experts. **Journal of the American Medical Association**. Vol. 242, 1979, p. 1279-1282.Disponível em: < https://jamanetwork.com/journals/jama/article-abstract/366606> Acesso em 10 Mai. 2021