REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

# A APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL NAS TÉCNICAS DE DEFESA E A ORQUESTRAÇÃO DE SISTEMAS CONTRA AMEAÇAS CIBERNÉTICAS

## *THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN DEFENSE TECHNIQUES AND THE ORCHESTRATION OF SYSTEMS AGAINST CYBER THREATS*

## *LA APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LAS TÉCNICAS DE DEFENSA Y LA ORQUESTACIÓN DE SISTEMAS CONTRA LAS CIBERAMENAZAS*

Eduardo Pereira Alves[1], Gustavo Lourenço da Silva[2], Diego Santos Almeida Pinto[3]

e6116919
https://doi.org/10.47820/recima21.v6i11.6919

PUBLICADO: 11/2025

**RESUMO**

Este trabalho apresenta uma análise aprofundada sobre a evolução das ameaças cibernéticas contemporâneas, tomando como ponto de partida o estudo de caso do grupo *hacktivista Anonymous Sudan*. O estudo investiga as motivações, estratégias e impactos globais de suas operações, com ênfase no uso de ataques DDoS (*Distributed Denial of Service*) para comprometer infraestruturas críticas e desestabilizar serviços essenciais. A pesquisa evidencia a crescente sofisticação desses ataques e a limitação das defesas tradicionais, como *firewalls* e sistemas de detecção baseados em assinaturas, diante de ameaças automatizadas e adaptativas. O objetivo central consiste em avaliar a eficácia das soluções de segurança baseadas em Inteligência Artificial (IA) e *Machine Learning* (ML) na mitigação de ataques distribuídos e massivos. A análise aborda a aplicação de algoritmos inteligentes capazes de identificar padrões anômalos e responder em tempo real, destacando o papel das plataformas SOAR (*Security Orchestration, Automation and Response*) na coordenação de ações automatizadas. Com base em revisão bibliográfica e documental, o estudo demonstra que a integração entre IA e cibersegurança representa um divisor de águas na defesa digital moderna. Conclui-se que a segurança cibernética atual se configura como uma disputa estratégica entre IA ofensiva e IA defensiva, em que a capacidade de aprendizado e adaptação dos sistemas é o fator determinante para garantir a resiliência digital e a continuidade operacional em ambientes críticos.

**PALAVRAS-CHAVE:** Cibersegurança. *Hacktivismo. Anonymous Sudan.* Inteligência Artificial. DDoS. SOAR.

***ABSTRACT***

*This study presents an in-depth analysis of the evolution of contemporary cyber threats through the case study of the hacktivist group Anonymous Sudan. It examines the group's motivations, strategies, and global impacts, focusing on the use of DDoS (Distributed Denial of Service) attacks to disrupt critical infrastructures and essential online services. The research highlights the increasing sophistication of these attacks and the limitations of traditional defense systems—such as firewalls and signature-based intrusion detectors—when facing automated and adaptive cyber operations. The main objective is to evaluate the effectiveness of Artificial Intelligence (AI) and Machine Learning (ML)-based security solutions in mitigating distributed and large-scale attacks. The study explores the application of intelligent algorithms capable of detecting anomalies and*

[1] Acadêmico cursando 4° período de Gestão da Tecnologia da Informação no Centro Universitário de Goiatuba.
[2] Acadêmico cursando 4° período de Gestão da Tecnologia da Informação no Centro Universitário de Goiatuba.
[3] Orientador: Professor do curso de Gestão da Tecnologia da Informação no Centro Universitário de Goiatuba.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



*responding in real time, emphasizing the role of SOAR (Security Orchestration, Automation and Response) platforms in coordinating automated defense mechanisms. Supported by a bibliographic and documentary review, the research demonstrates that the integration of AI into cybersecurity marks a new era in digital defense. The findings indicate that modern cybersecurity has become a strategic battle between offensive and defensive AI, where adaptability, automation, and continuous learning are essential to ensure digital resilience and operational continuity in critical environments.*

***KEYWORDS:*** *Cybersecurity. Hacktivism. Anonymous Sudan. Artificial Intelligence. DDoS. SOAR.*

***RESUMEN***
*Este trabajo presenta un análisis detallado sobre la evolución de las amenazas cibernéticas contemporáneas, tomando como estudio de caso al grupo hacktivista Anonymous Sudan. Se examinan sus motivaciones, estrategias e impactos globales, con énfasis en el uso de ataques DDoS (Distributed Denial of Service) para afectar infraestructuras críticas y servicios esenciales. La investigación evidencia la creciente sofisticación de estas ofensivas y las limitaciones de las defensas tradicionales, como los firewalls y los sistemas de detección basados en firmas, frente a amenazas automatizadas y adaptativas.El objetivo principal es evaluar la eficacia de las soluciones de seguridad basadas en Inteligencia Artificial (IA) y Machine Learning (ML) en la mitigación de ataques distribuidos y masivos. Se analiza la aplicación de algoritmos inteligentes capaces de detectar patrones anómalos y responder en tiempo real, destacando el papel de las plataformas SOAR (Security Orchestration, Automation and Response) en la automatización y coordinación de las defensas. Mediante una revisión bibliográfica y documental, el estudio demuestra que la integración de la IA en la ciberseguridad marca una nueva etapa en la defensa digital moderna.Se concluye que la seguridad cibernética actual constituye una competencia estratégica entre IA ofensiva e IA defensiva, donde la capacidad de aprendizaje y adaptación de los sistemas resulta esencial para garantizar la resiliencia digital y la continuidad operativa en entornos críticos.*

***PALABRAS CLAVE:*** *Ciberseguridad. Hacktivismo. Anonymous Sudan. Inteligencia Artificial. DDoS. SOAR.*

## INTRODUÇÃO

A segurança de sistemas é o pilar fundamental para a operação contínua e a credibilidade de qualquer organização na sociedade digital moderna. Este campo de estudo abrange a proteção de ativos digitais, garantindo sua confidencialidade, integridade e disponibilidade (CID), e constitui o principal desafio da tecnologia da informação na atualidade. A dependência crescente de infraestruturas conectadas torna qualquer falha de segurança uma ameaça direta à estabilidade econômica e social, justificando a urgência em pesquisas aprofundadas sobre o tema.

O crescente poder de grupos hacktivistas e cibercriminosos tem exposto de forma crítica a vulnerabilidade global. O caso do grupo *Anonymous Sudan* serve como um exemplo recente e impactante, notório por direcionar seus ataques de DDoS (*Distributed Denial of Service*) contra serviços essenciais, como bancos, telecomunicações e plataformas governamentais em diversos países. Tais ações demonstram que a população e as empresas estão diretamente ligadas a essa ameaça, sofrendo com a interrupção de serviços e a perda de confiança. Os ataques orquestrados por grupos como o *Anonymous Sudan* causam um colapso na disponibilidade dos

sistemas, um dos pilares da segurança, resultando em prejuízos financeiros bilionários, danos reputacionais irreparáveis e, em casos mais graves, a paralisação de serviços de utilidade pública. Esta ameaça é exacerbada pela sofisticação e automação que a Inteligência Artificial (IA) pode conferir tanto aos atacantes quanto aos defensores, transformando o cenário da segurança em uma verdadeira corrida armamentista digital.

Neste contexto, esta pesquisa contribui ao analisar as deficiências das técnicas de defesa cibernética tradicionais frente à escalada dessas ameaças e, em contrapartida, ao avaliar a eficácia das soluções de segurança baseadas em IA. O trabalho busca fornecer um arcabouço teórico e prático para justificar a implementação de sistemas de defesa automatizados e inteligentes, essenciais para garantir a resiliência e a continuidade dos negócios contra o *hacktivismo* moderno.

Dessa perspectiva, percebe-se a necessidade de investigar a fundo a intersecção entre o *hacktivismo* de alta performance e as tecnologias de defesa de próxima geração. O tema central deste trabalho é a análise da sofisticação dos ataques de negação de serviço do grupo *Anonymous Sudan* e o papel crítico da Inteligência Artificial (IA) no aprimoramento das técnicas de defesa cibernética, com foco na mitigação de ameaças de sobrecarga e na garantia da disponibilidade dos sistemas.

Diante do exposto sobre a escalada e a automação das ameaças cibernéticas, surge o seguinte questionamento central: Como as técnicas de defesa cibernética baseadas em Inteligência Artificial (IA) estão se adaptando e mitigando a escala e a sofisticação dos ataques *Distributed Denial of Service* (DDoS) realizados por grupos hacktivistas?

O Objetivo Geral desta pesquisa é avaliar o impacto dos recentes ataques *Distributed Denial of Service* (DDoS) do *Anonymous Sudan* e analisar a eficácia das soluções de segurança de sistemas baseadas em Inteligência Artificial (IA) na mitigação dessas ameaças e na proteção de infraestruturas críticas.

Para alcançar o objetivo geral, são estabelecidos três Objetivos Específicos que são: (1) Descrever a evolução do *hacktivismo*, detalhando as táticas e o impacto do *Anonymous Sudan* em infraestruturas críticas; (2) Identificar as limitações das técnicas de segurança de sistemas tradicionais (*firewalls* e IDS baseados em assinaturas) frente a ataques de sobrecarga massivos e adaptáveis; e (3) Analisar o potencial da Inteligência Artificial e do *Machine Learning* na criação de perfis comportamentais de tráfego, essenciais para a detecção e resposta automatizada a ataques DDoS.

A Hipótese deste trabalho é que as técnicas de defesa cibernética baseadas em Inteligência Artificial (IA), como *Machine Learning* e sistemas SOAR (*Security Orchestration, Automation and Response*), são significativamente mais eficazes na mitigação de ataques DDoS sofisticados, como os realizados pelo *Anonymous Sudan*, do que as defesas tradicionais.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



Essa eficácia se deve à capacidade preditiva e de adaptação da IA/ML, que permite criar modelos comportamentais de tráfego em tempo real, detectando e bloqueando anomalias de sobrecarga antes que os servidores sejam comprometidos, superando a lentidão e a limitação dos sistemas baseados em assinaturas fixas.

O trabalho será conduzido por meio de uma revisão bibliográfica e pesquisa documental, utilizando relatórios de segurança de grandes empresas e artigos científicos que detalham os ataques do *Anonymous Sudan* e a aplicação de *Machine Learning* na cibersegurança.

A crescente complexidade dos ataques cibernéticos e a atuação de grupos hacktivistas como o *Anonymous Sudan* mostram que as defesas digitais precisam evoluir com urgência. As medidas tradicionais já não dão conta da dimensão e da sofisticação das ameaças atuais. Nesse contexto, a Inteligência Artificial surge como um divisor de águas. Com o uso de técnicas como *Machine Learning* e soluções SOAR, a segurança digital ganha novas formas de prever, identificar e responder a incidentes. Esses recursos permitem detecção em tempo real, reações automáticas e aprendizado contínuo, tornando as defesas muito mais adaptáveis. Além disso, a IA reduz o tempo entre o ataque e a resposta, o que é essencial para minimizar prejuízos e manter serviços críticos funcionando mesmo sob forte pressão.

Conclui-se, portanto, que integrar tecnologias de IA aos sistemas de defesa não é mais uma opção, mas uma necessidade estratégica. A automação inteligente fortalece a resiliência, protege ativos valiosos e mantém a confiança do público diante de um cenário digital cada vez mais ameaçador.

## 1. REFERENCIAL TEÓRICO

Esta seção tem como objetivo consolidar a base teórica que sustenta o desenvolvimento desta pesquisa, estruturada em torno de três eixos fundamentais: o contexto do *hacktivismo* contemporâneo, os fundamentos da segurança da informação e a integração das tecnologias de Inteligência Artificial (IA) e *Machine Learning* (ML) na defesa cibernética moderna. A interligação entre esses temas é essencial para compreender como a transformação digital, a globalização das redes e a crescente automação dos processos tecnológicos vêm remodelando o panorama das ameaças e das respostas no campo da cibersegurança. O primeiro eixo trata do *hacktivismo*, fenômeno que emerge da fusão entre o ativismo político e a cultura hacker. Diferente do cibercrime convencional, que tem como foco o ganho financeiro, o *hacktivismo* busca promover ideologias, protestos ou denúncias sociais por meio de ataques e invasões a sistemas digitais. Essa forma de ativismo digital ganhou força nas últimas duas décadas, acompanhando a expansão da internet e o aumento da interdependência entre governos, empresas e serviços baseados em tecnologia.

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



Grupos como o *Anonymous* e, mais recentemente, o *Anonymous Sudan*, têm se destacado por utilizar ferramentas cibernéticas como instrumentos de pressão política e religiosa, executando ações que vão desde o vazamento de informações até ataques de negação de serviço (DDoS) contra infraestruturas estratégicas. Essas operações evidenciam o novo poder do ciberespaço como arena de disputas ideológicas e geopolíticas, onde a visibilidade pública e o impacto social das ações são tão importantes quanto os danos técnicos causados.

O segundo eixo abrange os fundamentos da segurança da informação, tradicionalmente sustentados pelos princípios de Confidencialidade, Integridade e Disponibilidade (CID). Esses pilares formam a espinha dorsal das políticas e práticas de proteção digital e são amplamente aplicados em ambientes corporativos, institucionais e governamentais. No entanto, o avanço das ameaças cibernéticas e a sofisticação dos métodos de ataque têm revelado as limitações dos mecanismos convencionais, como *firewalls*, antivírus e sistemas de detecção baseados em assinaturas. Essas soluções, embora essenciais, têm se mostrado insuficientes diante de ataques automatizados e distribuídos, especialmente os de larga escala, como os DDoS. Além disso, o aumento do volume de dados, a migração para a computação em nuvem e a proliferação de dispositivos IoT (Internet das Coisas) ampliaram consideravelmente a superfície de exposição. Essa nova realidade exige estratégias mais dinâmicas e inteligentes de defesa, capazes de reagir e se adaptar com velocidade às constantes transformações do ambiente digital.

No terceiro eixo, destaca-se a aplicação da Inteligência Artificial e do *Machine Learning* na segurança cibernética, considerada uma das maiores inovações tecnológicas da atualidade. Por meio de modelos preditivos e de aprendizado contínuo, essas tecnologias permitem que os sistemas reconheçam padrões comportamentais e detectem anomalias com alta precisão, mesmo em cenários de tráfego intenso e complexo. Em especial, o *Machine Learning* supervisionado e não supervisionado tem sido aplicado na detecção de ataques DDoS, permitindo distinguir entre picos de acesso legítimos e sobrecargas artificiais geradas por *botnets*. A integração desses recursos com plataformas SOAR (*Security Orchestration, Automation and Response*) potencializa a automação das respostas, possibilitando que ações defensivas, como bloqueios de IPs e isolamento de servidores, ocorram em tempo real, reduzindo drasticamente o impacto dos incidentes.

Além de aumentar a eficiência das defesas, a IA tem transformado a postura das organizações de reativa para proativa, permitindo antecipar comportamentos maliciosos e fortalecer continuamente as políticas de segurança. Esse novo paradigma redefine a forma como as instituições protegem seus dados, integrando análise de *big data*, modelagem de ameaças e automação operacional em um ecossistema unificado de defesa digital. Contudo, o uso crescente de IA também traz desafios éticos e técnicos, como o risco de IA adversária, em que atacantes utilizam os mesmos recursos inteligentes para aprimorar suas ofensivas.

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



Assim, o cenário da cibersegurança contemporânea é caracterizado por uma constante batalha de aprendizado entre IA ofensiva e IA defensiva, tornando a inovação tecnológica tanto uma arma quanto uma necessidade de sobrevivência.

Dessa forma, o referencial teórico aqui desenvolvido busca oferecer uma visão abrangente sobre a evolução do ciberespaço como campo de conflito e inovação. Ao relacionar as dinâmicas do *hacktivismo*, as bases conceituais da segurança digital e as transformações impulsionadas pela Inteligência Artificial, esta seção estabelece o alicerce conceitual necessário para compreender como as novas tecnologias estão redefinindo as fronteiras entre ataque e defesa, bem como o futuro da resiliência digital em escala global.

### 1.1. *Hacktivismo*, DDoS e o Estudo de Caso *Anonymous Sudan*

O termo *hacktivismo* resulta da junção das palavras "*hacker*" e "ativismo", sendo usado para designar ações de invasão ou interferência digital com motivações políticas, ideológicas ou sociais. Diferente do cibercrime tradicional, cujo foco está no lucro financeiro, o *hacktivismo* busca chamar a atenção para causas específicas, usando a tecnologia como forma de protesto. Essa modalidade tem crescido significativamente nas últimas décadas, acompanhando a expansão da conectividade global e a dependência crescente de sistemas digitais por parte de governos e empresas. Dentro desse contexto, grupos hacktivistas se destacam pela capacidade de mobilização e pela complexidade técnica de suas ações. Um dos exemplos mais recentes e relevantes é o *Anonymous Sudan*, que ganhou notoriedade por realizar ataques massivos a instituições governamentais e organizações privadas em diferentes países. Embora o grupo alegue agir em defesa de causas religiosas e políticas, muitos especialistas o associam a interesses geopolíticos, dada a natureza coordenada e o alcance de suas ofensivas. Esses ataques causam interrupções significativas em serviços essenciais, como bancos, telecomunicações e portais governamentais.

Uma das principais técnicas utilizadas pelo *Anonymous Sudan* e outros grupos semelhantes é o ataque *Distributed Denial of Service* (DDoS). Esse tipo de ataque visa sobrecarregar um servidor, rede ou serviço com um volume excessivo de requisições simultâneas, tornando-o incapaz de responder a usuários legítimos. O DDoS pode ser realizado por meio de redes de bots (*botnets*), compostas por milhares de dispositivos infectados e controlados remotamente, que agem de forma coordenada. O impacto global dos ataques DDoS é vasto, atingindo desde pequenas empresas até infraestruturas críticas de países inteiros. Quando direcionados a sistemas governamentais ou serviços financeiros, esses ataques podem causar prejuízos milionários e até comprometer a segurança nacional. Além disso, o DDoS é frequentemente utilizado como distração para ocultar outras invasões, como roubo de dados e espionagem cibernética, o que torna sua detecção e mitigação ainda mais desafiadoras.

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



Além da sobrecarga técnica causada pelos ataques DDoS, o *hacktivismo* moderno se caracteriza pela dimensão simbólica e midiática de suas ações. Grupos como o *Anonymous Sudan* não apenas interrompem serviços, mas também transmite mensagens políticas e ideológicas, buscando mobilizar a opinião pública ou pressionar governos e corporações. Essa dimensão simbólica amplia o impacto do ataque, pois a repercussão midiática frequentemente ultrapassa o dano técnico direto, gerando debates sobre segurança, privacidade e governança digital. Outro aspecto relevante é a sofisticação crescente desses ataques, que agora podem ser orquestrados em múltiplos vetores simultaneamente, incluindo a combinação de DDoS volumétricos com exploração de vulnerabilidades de aplicação ou propagação de *malware*. Essa convergência de técnicas aumenta a dificuldade de defesa, exigindo estratégias integradas que combinem monitoramento em tempo real, análise comportamental e respostas automatizadas.

Além disso, os grupos hacktivistas modernos exploram cada vez mais redes sociais e plataformas públicas como ferramentas de coordenação e divulgação. As ações do *Anonymous Sudan*, por exemplo, demonstram como ataques cibernéticos podem ser acompanhados de campanhas de informação digital, aumentando o efeito psicológico e de pressão sobre alvos estratégicos. Esse fenômeno reforça a necessidade de abordagens multidisciplinares em cibersegurança, que considerem não apenas aspectos técnicos, mas também sociais e comunicacionais.

### 1.2. Fundamentos de Segurança e Limitações das Defesas Tradicionais

A segurança da informação se apoia em três pilares fundamentais: Confidencialidade, Integridade e Disponibilidade (CID). Esses princípios formam a base para qualquer política ou prática de segurança digital. A confidencialidade garante que as informações sejam acessadas apenas por pessoas autorizadas; a integridade assegura que os dados não sejam alterados indevidamente; e a disponibilidade garante que os sistemas e serviços estejam acessíveis sempre que necessário. Historicamente, a proteção de sistemas digitais se baseou em soluções como *firewalls*, sistemas de detecção de intrusos (IDS) e filtros baseados em regras estáticas. Embora tenham desempenhado um papel essencial, essas ferramentas apresentam limitações frente às novas formas de ataque. Os *firewalls* tradicionais operam com base em listas de permissão e bloqueio, o que os torna vulneráveis a ataques que simulam tráfego legítimo. Já os IDS baseados em assinaturas só conseguem identificar ameaças conhecidas, deixando os sistemas expostos a ataques inéditos.

Em ambientes corporativos e de infraestrutura crítica, essas limitações se tornam ainda mais evidentes. O crescimento do volume de dados, a adoção de serviços em nuvem e a proliferação de dispositivos IoT ampliaram a superfície de ataque. Diante disso, técnicas defensivas tradicionais, dependentes de intervenção humana e regras fixas, não conseguem

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



acompanhar a velocidade e a complexidade das novas ameaças. Esse cenário exige uma reavaliação das estratégias de defesa, abrindo espaço para soluções mais dinâmicas e autônomas baseadas em Inteligência Artificial.

Embora os pilares CID (Confidencialidade, Integridade e Disponibilidade) continuem sendo referência, a evolução das ameaças revela lacunas críticas nas implementações tradicionais. Por exemplo, a integridade dos dados, antes garantida por mecanismos de criptografia e controles de acesso, pode ser comprometida por ataques direcionados que manipulam fluxos de informação em tempo real, como injeções de comandos ou adulteração de pacotes em redes distribuídas. Da mesma forma, a confidencialidade enfrenta desafios com o crescimento de ambientes em nuvem e a proliferação de dispositivos IoT, onde dados sensíveis circulam por múltiplas camadas e protocolos. Ataques de interceptação, coleta massiva de logs e exploração de vulnerabilidades de firmware tornam os sistemas convencionais menos eficazes, exigindo novas camadas de proteção, como criptografia adaptativa e monitoramento contínuo.

Por fim, a disponibilidade, tradicionalmente protegida por redundância e balanceamento de carga, encontra dificuldades diante de ataques de larga escala e sofisticados. Estratégias de mitigação baseadas apenas em filtragem estática ou bloqueio de IPs não são mais suficientes, principalmente quando os atacantes utilizam *botnets* distribuídas globalmente, capazes de mascarar a origem do tráfego e contornar medidas reativas. Isso evidencia a necessidade de soluções inteligentes e adaptativas, capazes de reconhecer padrões em tempo real e reagir de forma autônoma.

### 1.3. Inteligência Artificial (IA) e *Machine Learning* (ML) na Defesa Cibernética

A aplicação de Inteligência Artificial (IA) e *Machine Learning* (ML) na segurança cibernética representa um avanço significativo no combate a ataques cada vez mais sofisticados e automatizados. Essas tecnologias permitem que sistemas de defesa aprendam com o comportamento dos dados e se adaptem continuamente, identificando padrões anômalos que indicam tentativas de invasão ou ataques em andamento.

Diferente dos métodos tradicionais, a IA não depende exclusivamente de assinaturas pré-definidas. Em vez disso, ela utiliza modelos preditivos capazes de reconhecer desvios sutis no tráfego de rede ou nas atividades dos usuários. Essa abordagem é especialmente eficaz na detecção de ataques DDoS, pois permite distinguir entre picos legítimos de tráfego como promoções online e sobrecargas artificiais geradas por *botnets*.

Além disso, o uso de perfis comportamentais cria uma linha de base do que é considerado “normal” em um sistema, identificando instantaneamente quando algo foge do padrão. Essa inteligência permite uma resposta rápida e precisa, reduzindo o tempo médio de detecção e

ISSN: 2675-6218 - RECIMA21

mitigação de incidentes. Em cenários críticos, essa agilidade pode ser a diferença entre um simples alerta e a paralisação completa de serviços essenciais.

Outro ponto relevante é a integração dos sistemas de IA com soluções de *Security Orchestration, Automation and Response* (SOAR). Essa tecnologia combina automação e coordenação entre diferentes ferramentas de segurança, permitindo respostas sincronizadas e em tempo real. Assim, quando um comportamento suspeito é detectado, o sistema pode automaticamente bloquear endereços IP, isolar servidores comprometidos e alertar as equipes

responsáveis. A convergência entre IA e segurança cibernética marca uma nova era na defesa digital. As organizações que adotam essas tecnologias ganham não apenas eficiência operacional, mas também uma postura proativa diante das ameaças. O futuro da segurança da informação dependerá cada vez mais da capacidade dos sistemas de aprender, adaptar-se e responder de forma inteligente aos desafios de um ambiente digital em constante evolução.

O uso de IA e ML vai além da simples detecção de anomalias. Algoritmos avançados permitem prever comportamentos futuros, identificar padrões emergentes de ataque e ajustar continuamente políticas de defesa. Técnicas de aprendizado por reforço, por exemplo, possibilitam que sistemas de segurança “experimentem” respostas diferentes em cenários simulados, otimizando estratégias de mitigação antes que incidentes reais aconteçam. Além disso, a integração com plataformas SOAR amplia a capacidade de coordenação e automação das respostas, reduzindo o tempo entre a detecção de um comportamento suspeito e a execução de ações corretivas. Isso inclui não apenas o bloqueio de tráfego malicioso, mas também a análise contextual de logs, o isolamento de sistemas comprometidos e a emissão de alertas para equipes de segurança, garantindo uma visão completa do incidente.

Outro ponto importante é o papel da IA na priorização de ameaças. Em ambientes de alto volume de tráfego e múltiplos alertas simultâneos, os modelos de *Machine Learning* podem classificar automaticamente incidentes segundo sua criticidade, direcionando recursos humanos e computacionais para os casos mais urgentes. Essa capacidade de triagem inteligente melhora a eficiência operacional e diminui a sobrecarga das equipes de segurança.

Por fim, o contínuo desenvolvimento de IA defensiva contrasta com o uso de IA ofensiva por grupos hacktivistas, estabelecendo uma “corrida armamentista” digital. A eficácia das soluções baseadas em IA depende da qualidade dos dados, da atualização constante dos modelos e da capacidade de adaptação frente a novas técnicas de ataque. Assim, a integração de *Machine Learning*, análise comportamental e automação torna-se indispensável para garantir a resiliência e a continuidade das operações em um cenário de ameaças cada vez mais complexas.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



## 2. MÉTODOS

A presente pesquisa adota uma abordagem qualitativa, de caráter descritivo e exploratório, voltada à compreensão aprofundada do *hacktivismo*, dos ataques DDoS e do papel das tecnologias de Inteligência Artificial (IA) e *Machine Learning* (ML) na defesa cibernética. Essa abordagem permite analisar o fenômeno sob múltiplas perspectivas, valorizando a interpretação de dados e contextos em vez de meras quantificações. Busca-se compreender não apenas as técnicas empregadas, mas também as motivações, os impactos e as respostas possíveis dentro de um cenário global de ameaças digitais.

O método central utilizado será a revisão bibliográfica sistemática aliada à pesquisa documental, permitindo a construção de uma base teórica sólida e contextualizada. A revisão abrangerá artigos científicos, relatórios técnicos, *white papers* e estudos de caso que tratam tanto da atuação de grupos hacktivistas quanto do desenvolvimento de mecanismos inteligentes de defesa. Essa combinação garante um equilíbrio entre o rigor acadêmico e a observação prática, possibilitando identificar tendências, lacunas e contribuições relevantes no campo da segurança cibernética.

A coleta de informações será realizada em bases de dados reconhecidas internacionalmente, como *IEEE Xplore, Scopus, Web of Science e ACM Digital Library*, além de repositórios nacionais e documentos governamentais. Complementarmente, serão incluídos relatórios de *vendors* de segurança como *Fortinet, Cisco, Kaspersky* e *Check Point* e publicações de órgãos como o CERT-BR e a ENISA. As palavras-chave utilizadas englobarão termos como *"DDoS mitigation"*, *"Machine Learning cybersecurity"*, *"SOAR automation"*, *"hacktivism"* e *"Anonymous Sudan"*, tanto em português quanto em inglês.

Serão incluídos estudos publicados nos últimos 12 anos, com prioridade aos 5 mais recentes, dada a rápida evolução tecnológica do tema. Entre os critérios de seleção, priorizar-se-ão documentos que apresentem metodologias claras, análises de desempenho e aplicações práticas de IA e ML em cenários de defesa cibernética. Materiais sem autoria identificada, de natureza opinativa ou sem respaldo técnico serão excluídos, garantindo a confiabilidade da amostra e a coerência científica da revisão. Após a busca inicial, será conduzido um processo de triagem dividido em três etapas: análise de títulos e resumos, eliminação de duplicidades e leitura completa dos estudos selecionados. Cada etapa será devidamente documentada, registrando os motivos de exclusão e assegurando a transparência metodológica. Esse cuidado visa permitir que outros pesquisadores possam reproduzir ou validar o processo, reforçando o caráter científico do estudo.

Os documentos selecionados serão submetidos a uma avaliação crítica de qualidade, considerando variáveis como o tipo de algoritmo empregado, os conjuntos de dados utilizados, as métricas de desempenho e o nível de validação experimental.

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



Serão observadas também limitações apontadas pelos próprios autores, além de comparações entre abordagens distintas. Essa etapa permitirá identificar quais técnicas apresentam maior potencial de aplicação prática em cenários reais de mitigação de ataques DDoS e orquestração automatizada de respostas (SOAR).

A extração e organização dos dados seguirão um roteiro padronizado, registrando informações como: autor, ano, tipo de publicação, objetivo do estudo, técnicas aplicadas, resultados obtidos, limitações reconhecidas e recomendações propostas. A partir dessa compilação, será construída uma matriz comparativa, facilitando a visualização das semelhanças e diferenças entre as abordagens. Essa sistematização também servirá como base para a análise temática e a síntese interpretativa dos resultados. O estudo dedicará uma seção à análise de casos reais de ataques atribuídos ao Anonymous Sudan, observando padrões de comportamento, alvos preferenciais e possíveis conexões políticas ou religiosas. Essa análise não se limitará à dimensão técnica, mas buscará relacionar os eventos à geopolítica digital contemporânea. A partir dessa perspectiva, será possível compreender como as tecnologias de defesa podem se alinhar às exigências de segurança de governos e empresas em ambientes de alta criticidade.

Também será conduzida uma análise comparativa entre soluções SOAR comerciais e modelos acadêmicos, investigando aspectos como desempenho, tempo de resposta, escalabilidade e integração com sistemas legados. Essa comparação ajudará a compreender as diferenças entre a teoria e a prática, destacando as barreiras que ainda limitam a adoção de sistemas baseados em IA no cotidiano das operações de segurança (SecOps). Em complemento, a metodologia abordará as questões éticas e legais que permeiam o uso de IA e ML na cibersegurança. Serão discutidas as implicações da coleta e do tratamento de dados sensíveis, a necessidade de conformidade com legislações como a LGPD, e os riscos de vieses algorítmicos que possam comprometer decisões automatizadas. Essa etapa tem o propósito de propor reflexões sobre responsabilidade, transparência e governança no emprego de sistemas inteligentes de defesa.

As limitações do estudo também serão explicitadas. Como se trata de uma pesquisa qualitativa fundamentada em fontes secundárias, reconhece-se que parte das informações sobre grupos como o *Anonymous Sudan* pode apresentar incertezas quanto à autoria ou à veracidade de dados divulgados. Além disso, a constante evolução das técnicas de ataque e defesa impõe a necessidade de atualização contínua, tornando algumas conclusões temporárias ou dependentes do contexto tecnológico vigente.

Por fim, a metodologia culminará em uma síntese crítica e integradora, que reunirá os principais achados, identificará lacunas de conhecimento e proporá direções futuras para pesquisas sobre o uso de IA na mitigação de ataques DDoS. Espera-se que os resultados sirvam como subsídio tanto para pesquisadores quanto para profissionais do setor, oferecendo uma visão

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



ampla sobre como a automação inteligente pode redefinir a segurança cibernética frente a ameaças cada vez mais complexas e coordenadas.

## 3. RESULTADOS E DISCUSSÃO

Este capítulo apresenta a análise dos achados obtidos ao longo da revisão bibliográfica e documental, organizada de modo a permitir uma compreensão ampla e crítica das dinâmicas que envolvem os ataques cibernéticos do grupo *Anonymous Sudan* e a evolução das respostas defensivas baseadas em Inteligência Artificial (IA). A proposta é evidenciar como a natureza, a escala e a motivação desses ataques desafiam os modelos tradicionais de segurança e, simultaneamente, impulsionam o avanço de novas abordagens automatizadas de defesa.

Inicialmente, observa-se que os ataques promovidos pelo *Anonymous Sudan* têm se destacado pelo seu caráter massivo, coordenado e altamente adaptativo, direcionando-se a infraestruturas críticas e plataformas digitais de grande visibilidade. Esses ataques, frequentemente classificados como DDoS (*Distributed Denial of Service*), não se limitam a sobrecarregar servidores, mas exploram vulnerabilidades específicas de protocolos de rede e camadas de aplicação. Tal comportamento revela uma sofisticação que transcende o simples ativismo digital, aproximando-se de estratégias cibernéticas com motivação política e geopolítica.

Os impactos desses eventos são amplos e mensuráveis. Diversos relatórios técnicos apontam para a interrupção de serviços financeiros, governamentais e de comunicação, gerando prejuízos econômicos e danos à credibilidade institucional. Esses incidentes evidenciam um gap significativo nas defesas convencionais, principalmente em relação à capacidade de detecção e resposta em tempo real. As soluções baseadas em listas estáticas de bloqueio, assinaturas de ataque e regras predefinidas demonstram limitação diante da mutabilidade constante dos vetores de ataque empregados por grupos como o *Anonymous Sudan*. Diante desse cenário, a pesquisa identificou que a integração de IA e ML na segurança cibernética emerge como uma resposta concreta e promissora. Os algoritmos de aprendizado supervisionado e não supervisionado vêm sendo aplicados para distinguir padrões de tráfego legítimo e malicioso, reduzindo significativamente o número de falsos positivos e aumentando a eficiência operacional dos sistemas de defesa. Além disso, o uso de redes neurais profundas, árvores de decisão e máquinas de vetor de suporte (SVM) tem se mostrado eficaz em ambientes dinâmicos e de grande volume de dados.

Um dos principais diferenciais observados é a capacidade de aprendizado contínuo desses modelos. Diferente dos sistemas estáticos, os mecanismos baseados em ML podem ajustar seus parâmetros conforme novas ameaças são identificadas, criando um ciclo de aprimoramento progressivo. Essa característica é essencial em cenários onde os atacantes

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



utilizam técnicas de evasão e mascaramento, como a fragmentação de pacotes e a manipulação de cabeçalhos HTTP, tornando-se praticamente invisíveis para defesas convencionais.

Paralelamente, as soluções de SOAR (*Security Orchestration, Automation and Response*) foram destacadas como componentes fundamentais para a automação da resposta a incidentes. Essas plataformas integram-se a sistemas de monitoramento e correlação de eventos, como SIEM (*Security Information and Event Management*), permitindo que respostas sejam executadas de forma orquestrada, sem a necessidade de intervenção humana constante. A pesquisa revelou que o uso conjunto de IA e SOAR resulta em redução significativa do tempo de resposta (MTTR-*Mean Time to Respond*), além de permitir ações preventivas com base em previsões probabilísticas geradas pelos algoritmos.

Ao contrastar os dois polos analisados os ataques de alta complexidade e as defesas inteligentes e adaptativas, percebe-se uma disputa constante pela vantagem temporal e informacional. Enquanto os agentes ofensivos se valem da velocidade de disseminação e da capacidade de sobrecarga, os sistemas de IA buscam alcançar a resposta quase instantânea, fundamentada em análise preditiva e correlação de dados em larga escala. O resultado é uma corrida tecnológica assimétrica, na qual pequenas inovações em um dos lados podem alterar substancialmente o equilíbrio cibernético.

Outro ponto de destaque é a viabilidade prática dessas tecnologias. Embora muitos estudos apresentem resultados promissores em ambientes controlados, a implementação em infraestruturas reais ainda enfrenta desafios, como a falta de padronização de *datasets*, os custos computacionais elevados e a necessidade de integração com sistemas legados. Além disso, a eficácia dos modelos de ML depende diretamente da qualidade e diversidade dos dados utilizados no treinamento, o que levanta questões sobre viés algorítmico e privacidade de informações sensíveis.

Do ponto de vista estratégico, a análise demonstra que a combinação entre IA, ML e SOAR tem potencial para redefinir completamente o paradigma de segurança cibernética. O conceito de resposta reativa dá lugar a uma defesa proativa e autônoma, em que sistemas são capazes de prever ameaças antes que causem danos efetivos. Essa mudança de perspectiva coloca a IA não apenas como uma ferramenta de suporte, mas como um agente decisório dentro do ecossistema de defesa digital. Finalmente, é possível afirmar que a discussão dos achados reforça a necessidade de uma sinergia entre pesquisa acadêmica e aplicação industrial, de modo que os avanços teóricos em aprendizado de máquina possam se converter em soluções práticas e escaláveis.

O caso do *Anonymous Sudan*, com sua combinação de ataque simbólico e técnico, exemplifica o desafio de proteger infraestruturas críticas em uma era de automação e hiperconectividade. Assim, o papel da IA e do ML torna-se não apenas uma alternativa viável, mas

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



uma necessidade estratégica para garantir a continuidade e a resiliência das operações no ciberespaço.

## 4. CONSIDERAÇÕES

A conclusão deste estudo reforça, de forma inequívoca, a tese de que a adoção de uma segurança robusta em sistemas Iot integrados com 5G/6G não constitui apenas uma tendência tecnológica passageira, mas um vetor crítico para o sucesso e a competitividade empresarial na era digital.

O estudo cumpriu o Objetivo Geral ao conduzir uma análise aprofundada dos benefícios e desafios, demonstrando que a implementação da segurança só é sustentável quando guiada por uma estratégia holística que equilibra a inovação tecnológica (IA, *Blockchain*) com a responsabilidade social, privacidade e ética.

A pesquisa forneceu uma resposta fundamentada ao Problema de Pesquisa, indicando que a implementação eficaz da segurança em IoT-5G/6G depende criticamente da superação dos desafios estruturais. A solução não está apenas na aquisição de *hardware* e *software*, mas na adoção de estratégias proativas, como o investimento contínuo na capacitação da força de trabalho (*reskilling* e *upskilling*) e a incorporação da governança ética (*AI Ethics*) desde a fase de concepção do projeto. Dessa forma, mitiga-se o risco de vieses algorítmicos e garante-se a *accountability*.

O principal aporte científico deste artigo reside na síntese analítica das estratégias de segurança distribuída, que servem como um roteiro inicial para gestores. Esta análise alinha os benefícios de resiliência com as exigências de conformidade legal (LGPD/GDPR). Como sugestão para estudos futuros, recomenda-se a realização de uma pesquisa de campo, com entrevistas ou *surveys* em empresas brasileiras de diferentes portes e setores de atuação (e.g., financeiro vs. varejo), para quantificar o Retorno sobre o Investimento (ROI) das tecnologias de segurança baseadas em IA e *Blockchain* na prevenção de incidentes e validar, com dados primários, a eficácia das estratégias de *reskilling* e adoção ética propostas neste trabalho.

## REFERÊNCIAS

AL-GARADI, M. A. *et al.* A survey of machine learning techniques for cyber security in IoT**. IEEE Communications Surveys & Tutorials**, v. 20, n. 3, p. 2577-2601, third quarter 2018.

ANDREWS, P. V.; CHERIAN, J.; MADY, M. F. A Survey on the Use of Blockchain in the Internet of Things (IoT) Security. **International Journal of Computer Networks and Communications**, v. 14, n. 4, p. 75-87, 2022.

BECKER, S.; KUNZE, C.; VANCEA, M. Community energy and social entrepreneurship: Addressing purpose, organization and embeddedness of renewable energy projects. **Journal of Cleaner Production**, v. 147, p. 25–36, 2017.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



BOUSSAHA, H. et al. 5G/6G Security Challenges and Solutions for IoT: A Survey. **IEEE Access**, v. 11, p. 11883-11910, 2023.

BRYNJOLFSSON, E.; MCAFEE, A. **The second machine age**: Work, progress, and prosperity in a time of brilliant technologies. New York: W. W. Norton & Company, 2014.

DAVENPORT, T. H.; RONANKI, R. Artificial intelligence for the real world. **Harvard Business Review**, v. 96, n. 1, p. 108-116, 2018.

MERCADO COMUM DO SUL (MERCOSUL). **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

SHAFI, M. *et al*. 6G Vision: A New Era of Wireless Communication. **Applied Sciences**, v. 10, n. 12, p. 4390, 2020.

YIN, H. *et al.* Security and Privacy in 5G-Enabled Internet of Things: Challenges and Solutions. **IEEE Network**, v. 34, n. 4, p. 28-34, July/August. 2022.

**ISSN: 2675-6218 - RECIMA21**