Faculdades Integradas IESGO	**Proposta de Tema**	**NOTA:**
Curso: Sistema de Informação		
Data de entrega: 26/02/2026	**Sem:** 1º/2026	
DISCIPLINA: Práticas Orientadas de TCC		
ORIENTADOR OR (A): Sandir Campos	**E-MAIL:** sandir.campos@iesgo.edu.br	
ALUNO (A): Pablo Soares da Silva	**E-MAIL:** pablosoares1204@gmail.com	

Português:

O Impacto da Inteligência Artificial na Cibersegurança: O Dilema entre a Defesa Automatizada e a Sofisticação dos Ataques.

Resumo:

Este artigo busca analisar a natureza ambivalente da Inteligência Artificial (IA) no cenário da segurança digital contemporânea. Por um lado, a IA surge como uma segurança adicional indispensável, permitindo a detecção de anomalias em tempo real, automação de respostas a incidentes e análise preditiva de vulnerabilidades com uma velocidade superior à capacidade humana. Por outro viés, a tecnologia tem sido explorada para viabilizar ataques mais sofisticados, como phishing altamente personalizado via modelos de linguagem (LLMs), criação de deepfakes para engenharia social e o desenvolvimento de malwares polimórficos que evadem sistemas tradicionais. Além da automatização do processo de modificação e disseminação de Malwares e Vírus.

O objetivo deste artigo é investigar como o equilíbrio de forças entre atacantes e defensores está sendo redefinido por essas ferramentas. Através de uma revisão bibliográfica e análise de casos recentes, o estudo buscará responder se a **IA** está tornando o ecossistema digital mais seguro ou se está apenas escalando a corrida armamentista cibernética. A pesquisa justifica-se pela necessidade crítica de organizações e governos adaptarem suas infraestruturas diante de ameaças cada vez mais autônomas e imprevisíveis. Dificultando o controle e saúde dos sistemas.

Palavras-chave para o artigo:

- Inteligência Artificial;
- Cibersegurança;
- Machine Learning;
- Cibercrime;
- Defesa Digital.

Inglês:

The Impact of Artificial Intelligence on Cybersecurity: The Dilemma Between Automated Defense and Sophisticated Attacks.

Summary:

This article seeks to analyze the ambivalent nature of Artificial Intelligence (AI) in the contemporary digital security landscape. On the one hand, AI emerges as an indispensable additional security measure, enabling real-time anomaly detection, automated incident response, and predictive vulnerability analysis at a speed superior to human capabilities. On the other hand, the technology has been exploited to enable more sophisticated attacks, such as highly personalized phishing via language models (LLMs), the creation of deepfakes for social engineering, and the development of polymorphic malware that evades traditional systems. This also includes the automation of the process of modifying and disseminating malware and viruses.

The objective of this article is to investigate how the balance of power between attackers and defenders is being redefined by these tools. Through a literature review and analysis of recent cases, the study will seek to answer whether AI is making the digital ecosystem safer or if it is merely escalating the cyber arms race. The research is justified by the critical need for organizations and governments to adapt their infrastructures in the face of increasingly autonomous and unpredictable threats, making it difficult to control and maintain the health of systems.

Keywords for the article:

- Artificial intelligence;
- Cybersecurity;
- Machine Learning;
- Cybercrime;
- Digital Defense;