

Artificial Intelligence Threats & Opportunities for Cybersecurity

How AI Could Pose a Threat to Cybersecurity?



Gülhan Ertürk Akgül

arvis[®]
olo
teknoloji

11.02.2025



Artificial Intelligence Threats to Cybersecurity

Agenda

- How AI is Used in Cyber Threats
- Automated Attacks and Vulnerabilities
- Deepfake Attacks & Social Engineering
- AI-Powered Phishing Attacks
- Data Privacy Risks & AI-Driven Surveillance
- Malicious AI Chatbots & Malware Generation
- AI in Defense, Attack
- Real-World Case Studies
- Strategies & Future
- Examples



Artificial Intelligence Threats to Cybersecurity

- The development of artificial intelligence in recent years has brought some challenges as well as benefits to cybersecurity.
- The capabilities of artificial intelligence are promising for the defense field.
- But, they can also be exploited by malicious people in different areas.
- AI can pose very important threats.



olo AI's Role in Cyber Threats

Automation

- AI can automate attacks, making them faster and more efficient.
- It can also analyze large datasets to identify vulnerabilities and exploit them.

Adaptability

- AI systems can learn and adapt, making them capable of circumventing traditional security measures.
- AI-powered attacks can evolve and change over time, making them harder to detect and defend against.

Defense

- AI is employed in cybersecurity defense systems for:
 - Threat detection
 - Anomaly detection
 - Proactive threat hunting
 - Automated security response

Attack

- Cybercriminals are leveraging AI to:
 - Automate attacks
 - Target vulnerabilities
 - Bypass security measures
 - Generate sophisticated malware.

olo Automated Attacks and Vulnerabilities

1. Vulnerability Scanning

- AI algorithms rapidly scan systems for vulnerabilities and weaknesses, identifying potential attack vectors.
- AI can scan systems for vulnerabilities, quickly identify weaknesses, and exploit them for unauthorized access or data theft.



Automated Attacks

2. Automated Botnets

- Large-scale botnets powered by AI execute coordinated attacks against multiple targets, overwhelming defenses.
- AI-powered botnets can launch large-scale attacks, overwhelming systems and causing significant damage.
- These bots can coordinate their actions and adapt their strategies to evade detection.

olo Automated Attacks and Exploitation of Vulnerabilities

3. Brute Force Attacks

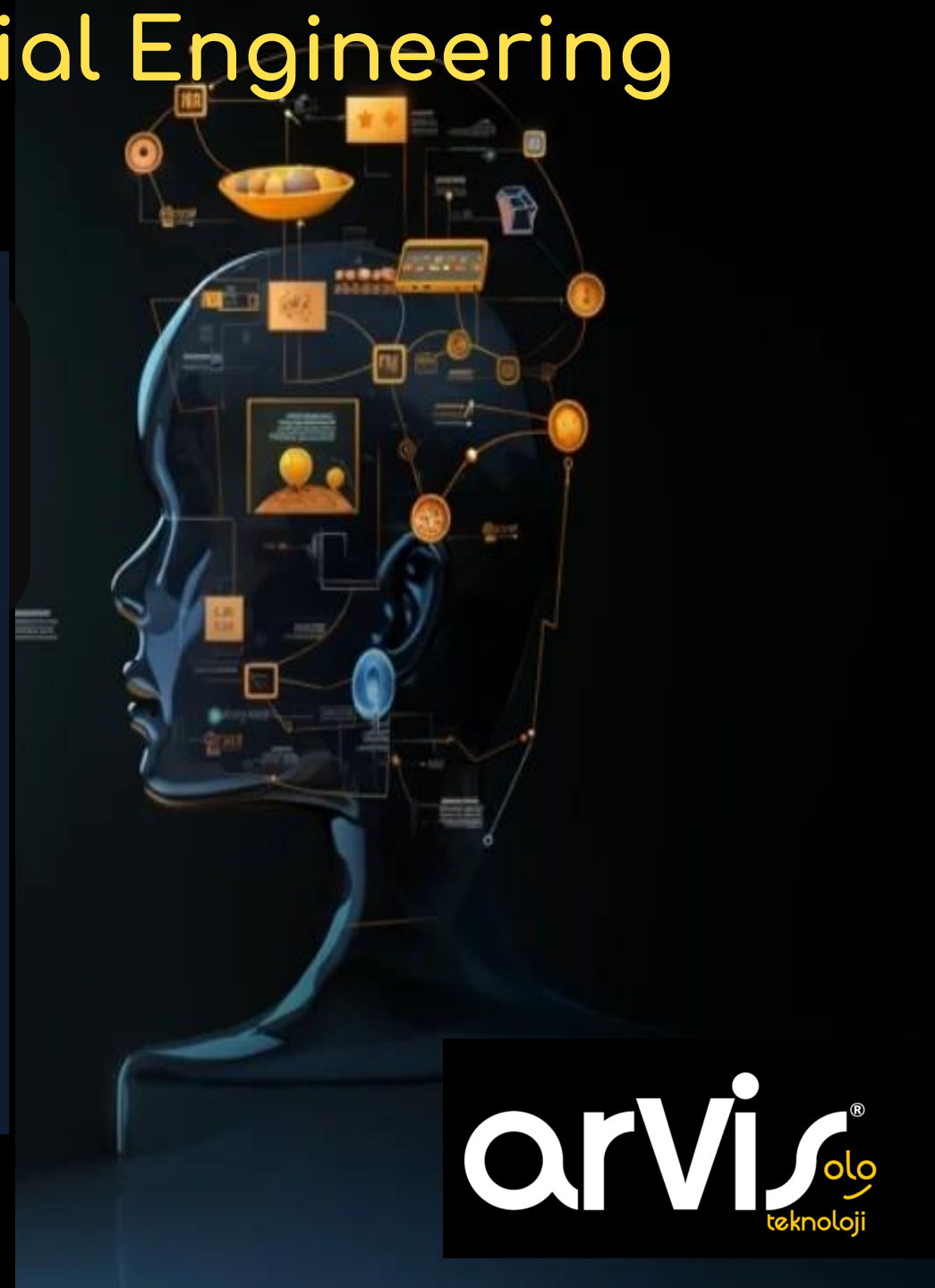
- AI-assisted brute force attacks use sophisticated algorithms to crack passwords and gain unauthorized access to systems.



olo Deepfake Attacks and Social Engineering

Deepfakes

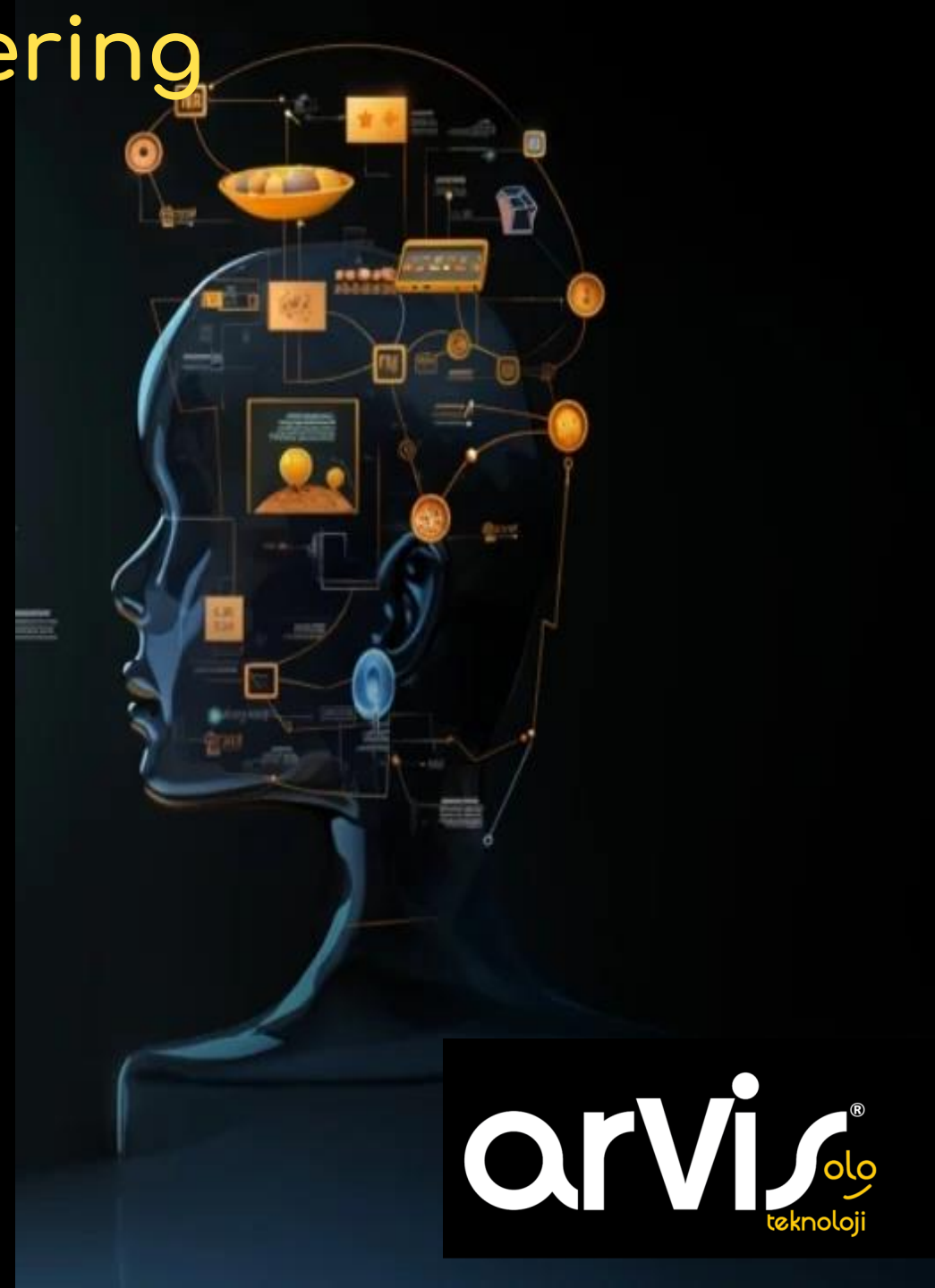
- AI-generated synthetic media including videos and audio, can be used to impersonate individuals, deceive authentication systems, and spread misinformation.
- AI can be used to create deepfakes, including fake videos and audio recordings for frauds.
- Deepfakes can be used to manipulate people and business.



olo Deepfake & Social Engineering

Social Engineering

- AI-powered tools are employed for highly personalized phishing emails and other social engineering attacks, exploiting human trust and vulnerabilities.



olo AI-Powered Phishing Attacks



Personalized Phishing

AI analyzes data to create highly targeted phishing emails, mimicking legitimate communications and increasing the likelihood of user deception.



Bypass Security

AI-generated phishing emails are harder to detect due to advanced natural language processing techniques, circumventing traditional spam filters.



Business Email Compromise

AI-powered BEC scams exploit human error by impersonating executives or business contacts, leading to financial losses through fraudulent wire transfers.



Emails Designed in
Inttp of fakes (email) and



Spam

Iusnow hestam add
fake gmat you:

Phare ion fagaik, sam, Lare t, d
Disprove your/glaws/ Links you
effter/Lnot allg suspicious
suspous link>

olo AI-Powered Phishing Attacks

Personalized Phishing

- AI can generate highly personalized phishing emails, making them more likely to be opened and clicked on by unsuspecting victims.

Advanced Language Processing

- AI's ability to mimic human language makes it difficult to detect AI-generated phishing messages.
- These messages can appear authentic and even conversational.



olo Data Privacy Risks and AI-Enhanced Surveillance

AI-powered data mining can reveal sensitive user information, potentially leading to privacy breaches and identity theft.



olo AI-Driven Surveillance & Privacy

Data Mining

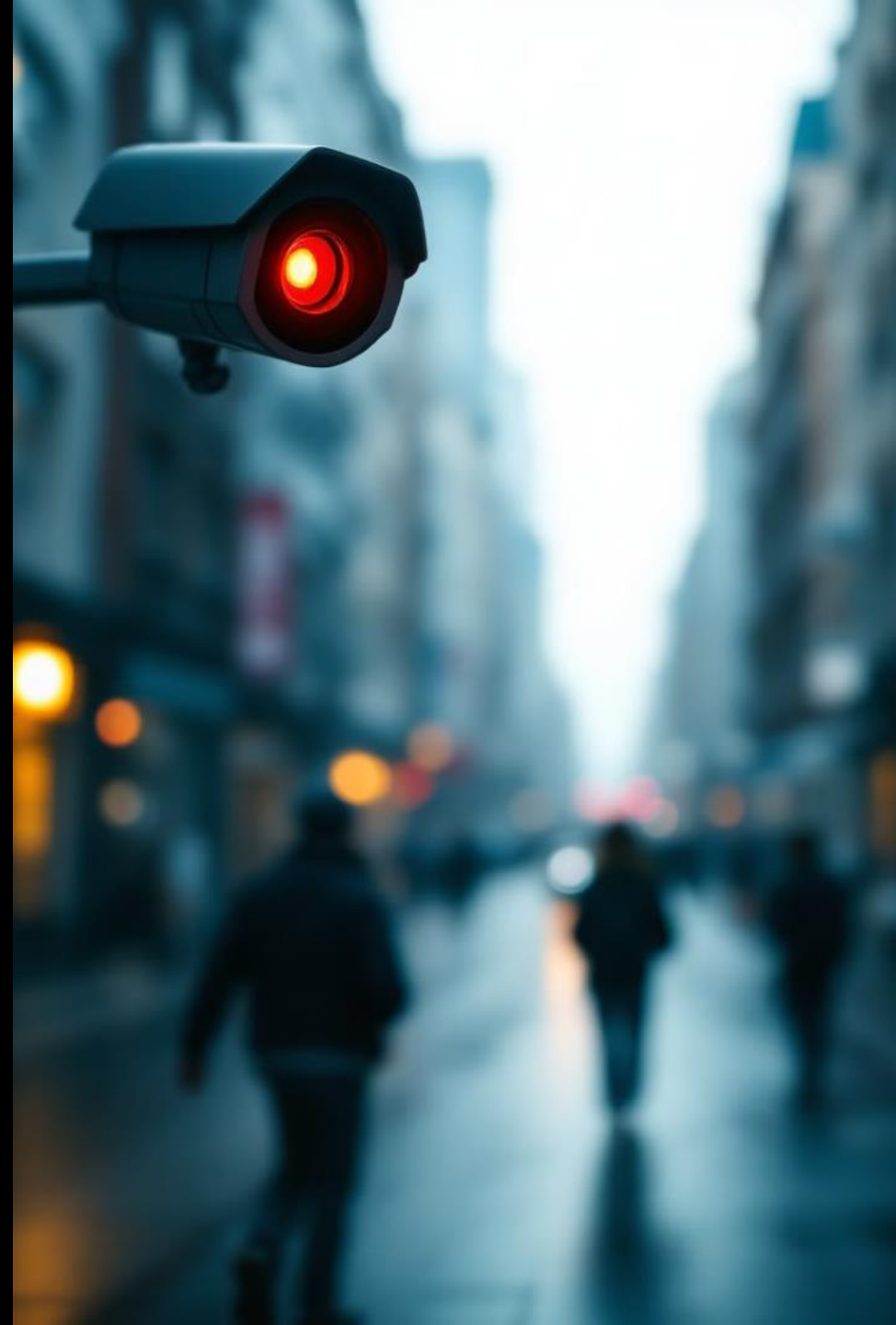
- AI-powered data mining algorithms can extract sensitive personal information from large datasets, posing significant privacy risks.

Mass Surveillance

- AI-driven facial recognition and other surveillance technologies enable mass monitoring of individuals in public spaces, raising concerns about privacy violations.

Privacy Breaches

- The vast amount of data collected by AI-powered systems is vulnerable to breaches, potentially exposing sensitive information to malicious actors.



olo AI Chatbots & Malware Generation

Deceptive Chatbots

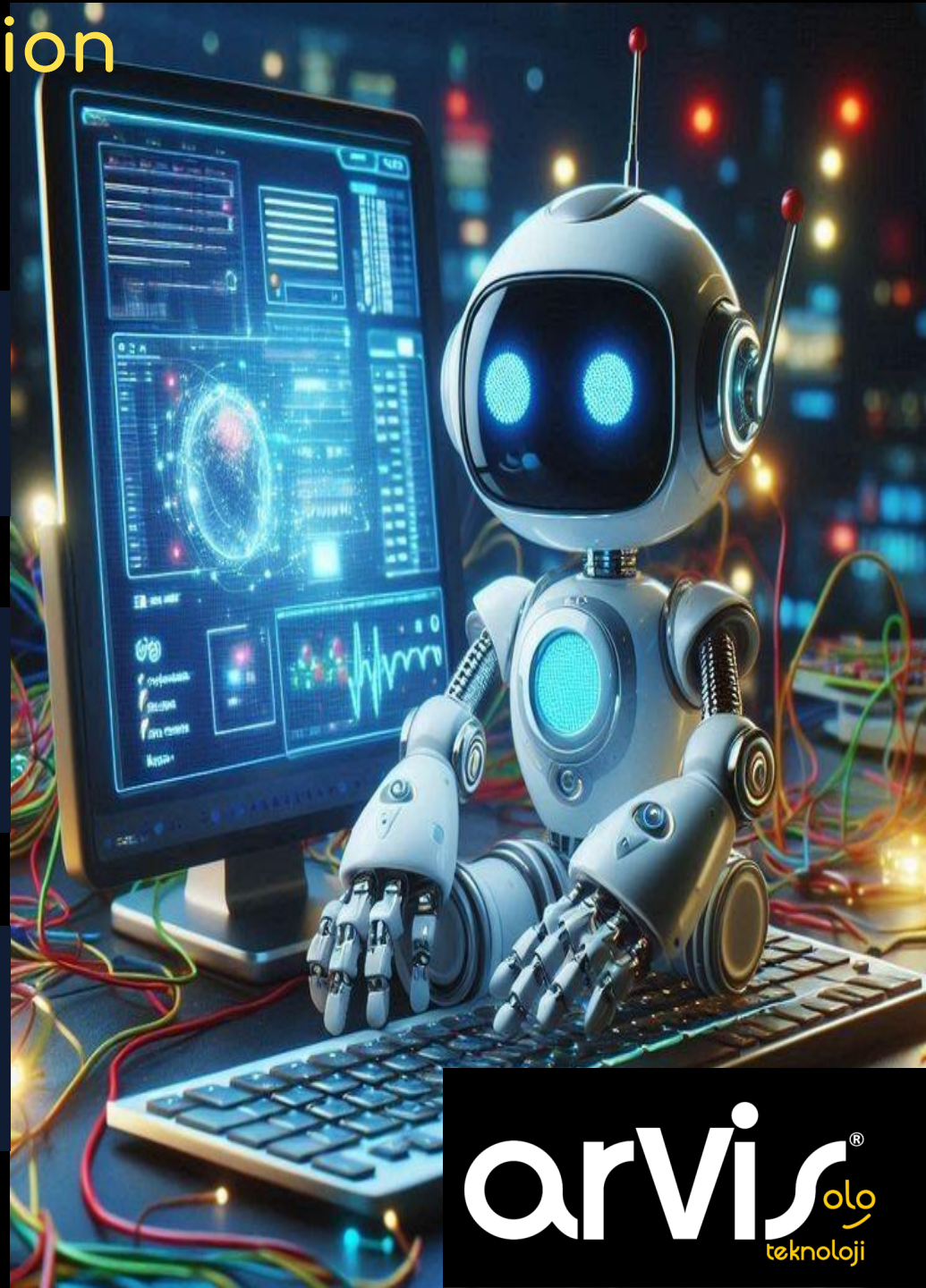
- AI-generated chatbots can impersonate human agents, engaging in conversations to trick users into providing sensitive data or installing malware.

Evolving Malware

- AI algorithms can generate undetectable malware variations, evading traditional security software and making detection and remediation challenging.

Ransomware

- AI-powered ransomware is constantly evolving, becoming more sophisticated and difficult to decrypt, leading to significant financial losses.



Malicious AI Chatbots and Malware Generation



AI-generated chatbots can trick users into divulging sensitive information or downloading malicious software.

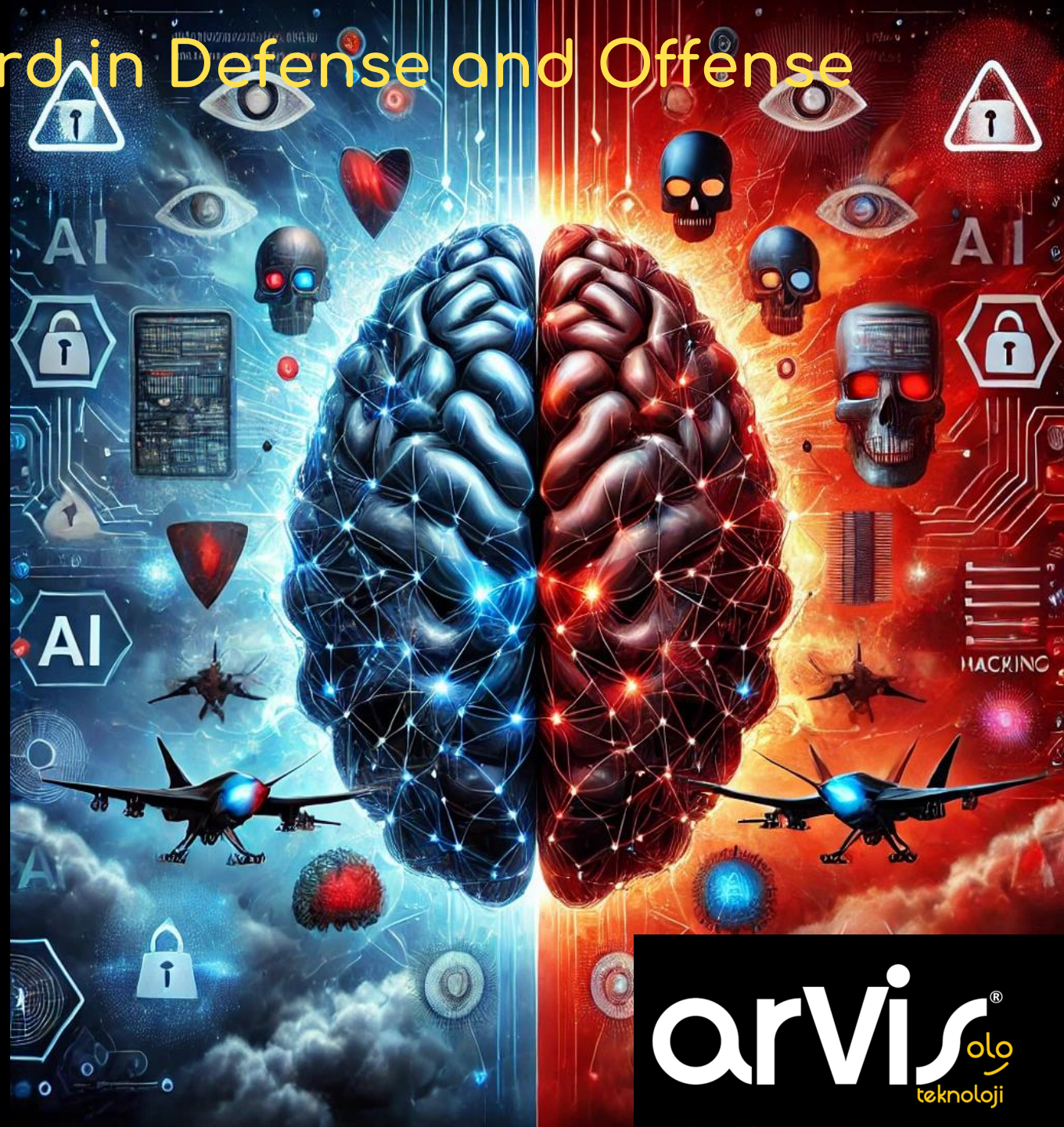


AI can create new types of malware that are difficult to detect and remove.



AI: A Double-Edged Sword in Defense and Offense

- AI is increasingly used for cybersecurity defense, including threat detection, anomaly detection, and incident response.
- However, attackers are also using AI to circumvent security mechanisms and launch more sophisticated attacks.
- This creates a constant arms race, where both defenders and attackers leverage AI to gain an advantage.



olo Mitigating AI Threats: ?

Proactive Approachs

1. AI Threat Detection

- Organizations need to implement AI-driven threat detection and response systems to identify and mitigate AI-driven attacks.

2. Ethical AI Development

- Promoting ethical AI development and responsible use is crucial to prevent the misuse of AI for malicious purposes.

3. Continuous Learning

- Continuous learning and adaptation are essential to stay ahead of the constantly evolving AI threat landscape.

4. Proactive Defense

- Organizations must proactively invest in AI-based security solutions and adopt a layered security approach to defend against AI-driven threats.



- Stronger AI-Powered Defense Systems
- Human-AI Collaboration
- Ethical AI and Regulations
- Continuous AI Training
- Cyber Awareness and Training





Future - AI Opportunities

- Stronger Defense Systems
- Automatic and Intelligent Response Systems
- Attack Prediction and Prevention
- Advanced Authentication
(face recognition, voice recognition)
- Cybersecurity Job Opportunities





Examples

QueenBee



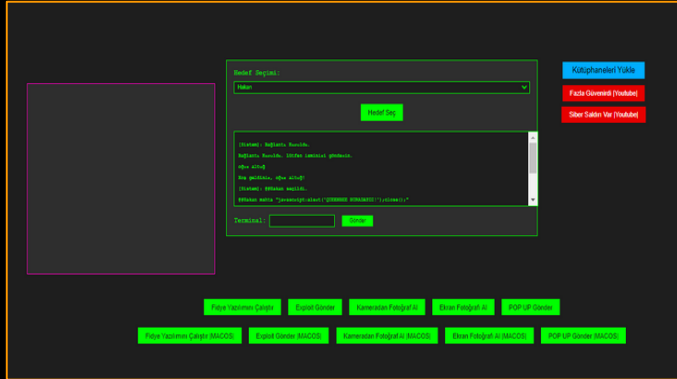
arVis[®]
olo
teknoloji



Examples

QueenBee

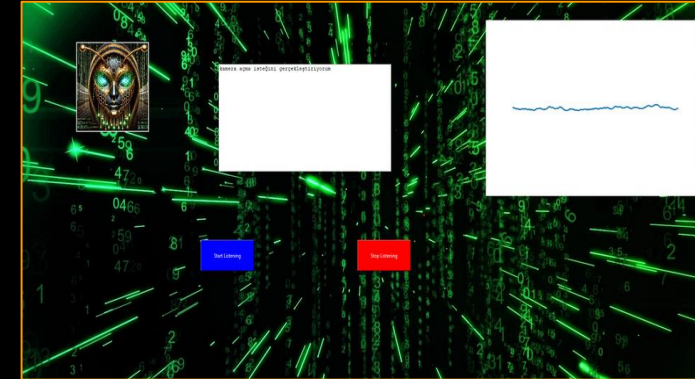
Attack



QueenNet



HorNet



AyQueen

Defense



DefQueen



Examples

QueenBee

```
virüslüdeneme.py > ...
1 import tensorflow as tf
2 import numpy as np
3 import matplotlib.pyplot as plt
4 from tensorflow.keras.preprocessing import image as keras_image
5 import cv2
6 from tensorflow.keras.models import load_model
7 from skimage.metrics import structural_similarity as ssim
8 from denoising_diffusion_pytorch.cnn_gaussian_diffusion import Denoising_Aided_Convolutional_Neural_Network
9
10 import logging
11
12 logging.basicConfig(level=logging.ERROR)
13
14
15
16 def load_image(image_path):
17     image = cv2.imread(image_path).astype(np.float32)/255
18     image = cv2.cvtColor(image, cv2.COLOR_BGR2RGB)
19     image = cv2.resize(image, (128, 128))
20
21     return image
22
23 image_path = 'normaldog.jpg'
```

PROBLEMS 2 OUTPUT DEBUG CONSOLE TERMINAL PORTS

PS C:\Users\Hakan\Desktop\siber_son>

Thanks...

arvis[®]
olo
teknoloji

ARVIS Teknoloji San. Tic. A.Ş.

Teknopark İstanbul Cube Incubation
Sanayi Mah. Teknopark Bulvarı No:1/4C
34906 Pendik/İstanbul



arvis-technology



ArvisTeknoloji



arvisteknoloji



ArVis-Teknoloji

Tel : +90 530 122 78 43
info@arvis.com.tr
www.arvis.com.tr