Harnessing the Power of AI

Unleashing the Defensive and Offensive Capabilities in Cybersecurity

May 16th, 2024

Overview and History of Artificial Intelligence Usage

Iowa Communications Alliance

VantagePoint EMPLOYEE OWNED

1

About the Presenter

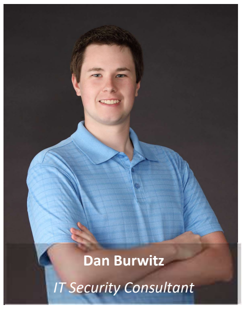
Jerad Glore – IT Security Specialist

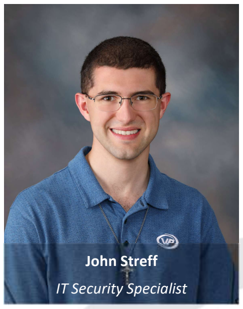
- Started at VPS in 2023
- Areas of Focus (Telecommunications)
  - Penetration Testing
  - Social Engineering
  - IT Audit
- Missouri State University
  - BS Information Technology (Emphasis in Cybersecurity)
- Jerad.Glore@vantagepnt.com

2

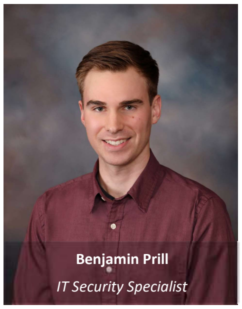
Meet the Security Team

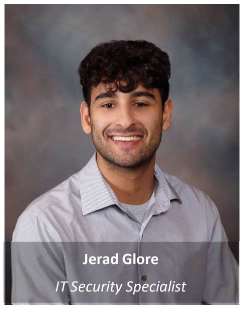
James Taylor
Sr. IT Security Consultant

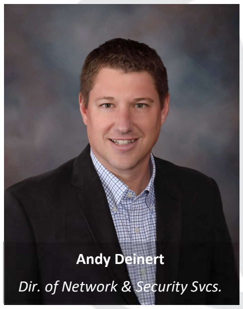

Dan Burwitz
IT Security Consultant


John Streff
IT Security Specialist

William Gonzalez
IT Security Specialist


Benjamin Prill
IT Security Specialist


Jerad Glore
IT Security Specialist


Andy Deinert
Dir. of Network & Security Svcs.

Josh Tollefson
Sr. IT Audit Consultant

3

Vantage Point Solutions, Mitchell, SD.

www.vantagepnt.com

4

VPS serves **hundreds of clients**, large and small, across the country and internationally.

5

Here for all your questions

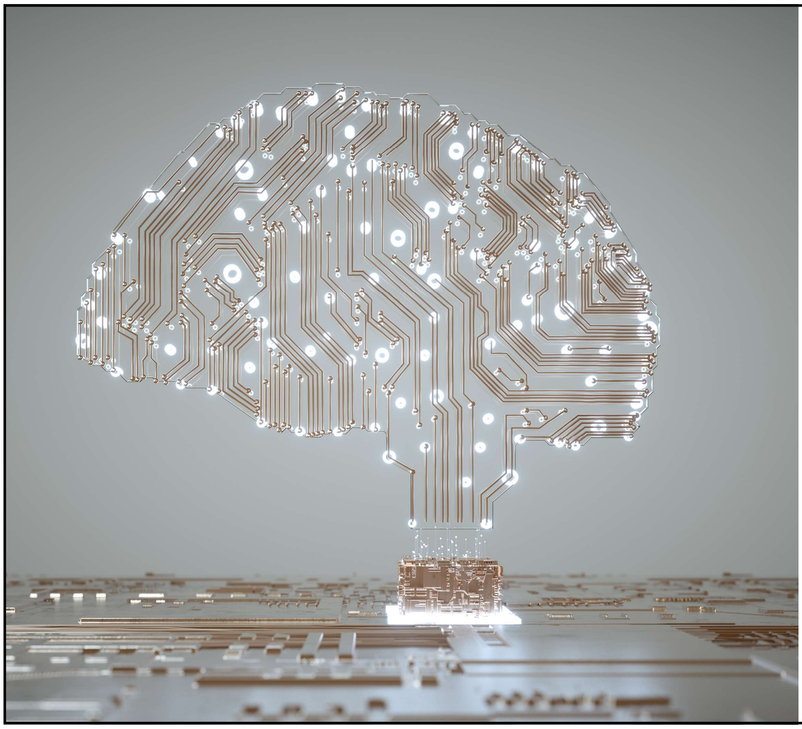
- ENTERPRISE RISK MANAGEMENT
- AUDIT
- REGULATORY COMPLIANCE
- INDEPENDENT CREDIT REVIEW
- CYBERSECURITY
- NETWORK MONITORING
- SERVER VIRTUALIZATION
- DATA NETWORKING

6

Today's Objectives

- Define Artificial Intelligence (AI)
- History
- Examples
- Challenges

7



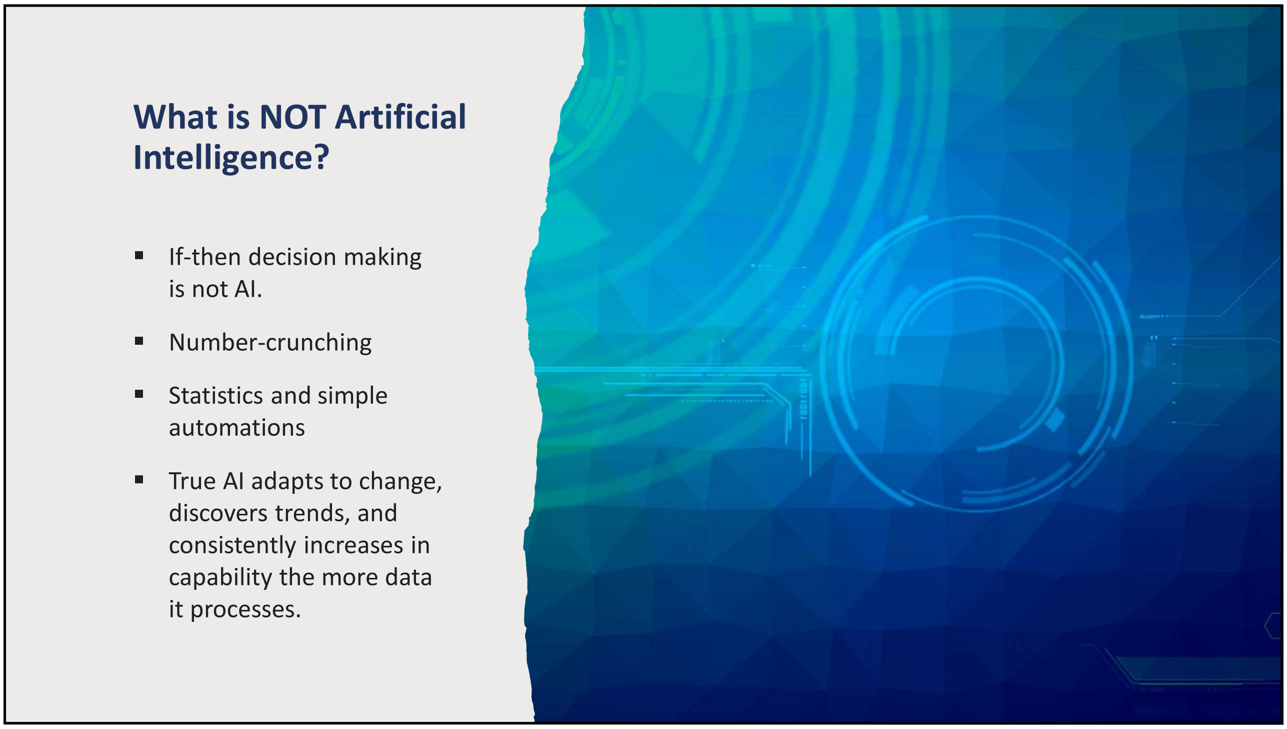
What is Artificial Intelligence?

- "A branch of computer science dealing with the simulation of intelligent behavior in computers."
- "The capability of a machine to imitate intelligent human behavior."

-Merriam-Webster

Notice that it is only a "simulation" or an "imitation" of intelligent behavior.

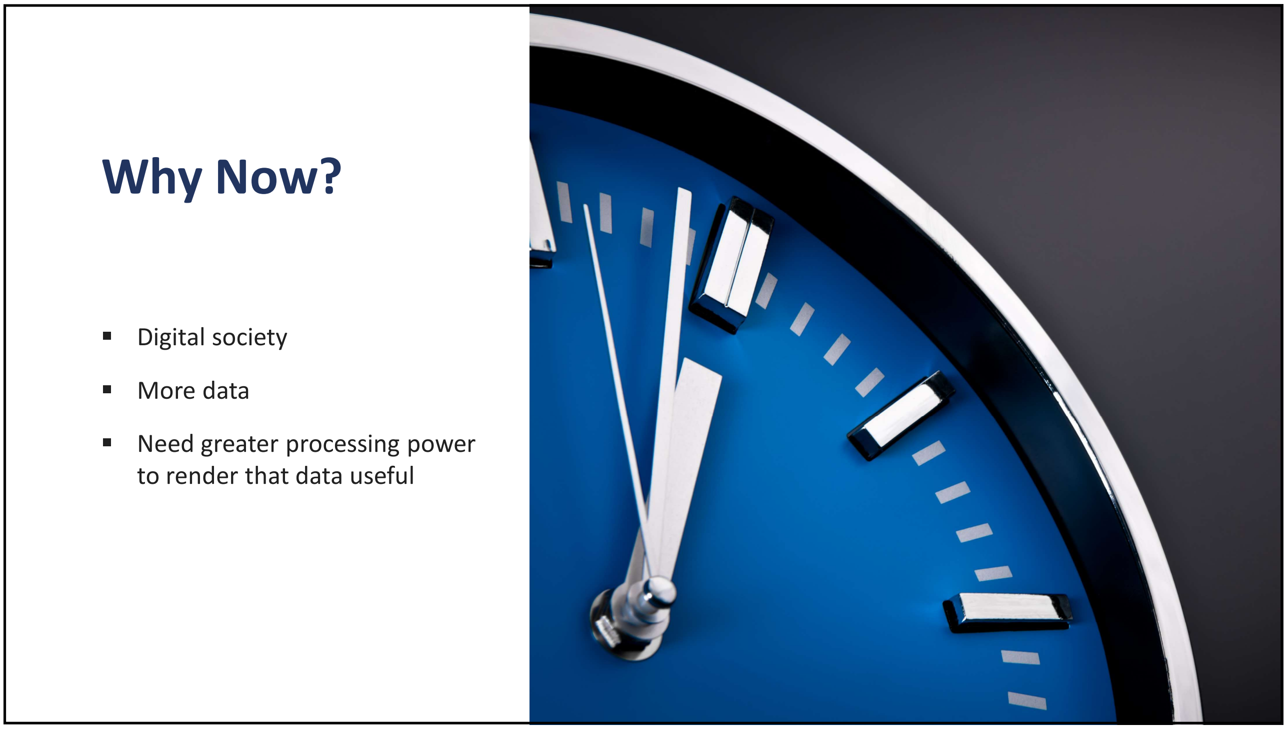
8



What is NOT Artificial Intelligence?

- If-then decision making is not AI.
- Number-crunching
- Statistics and simple automations
- True AI adapts to change, discovers trends, and consistently increases in capability the more data it processes.

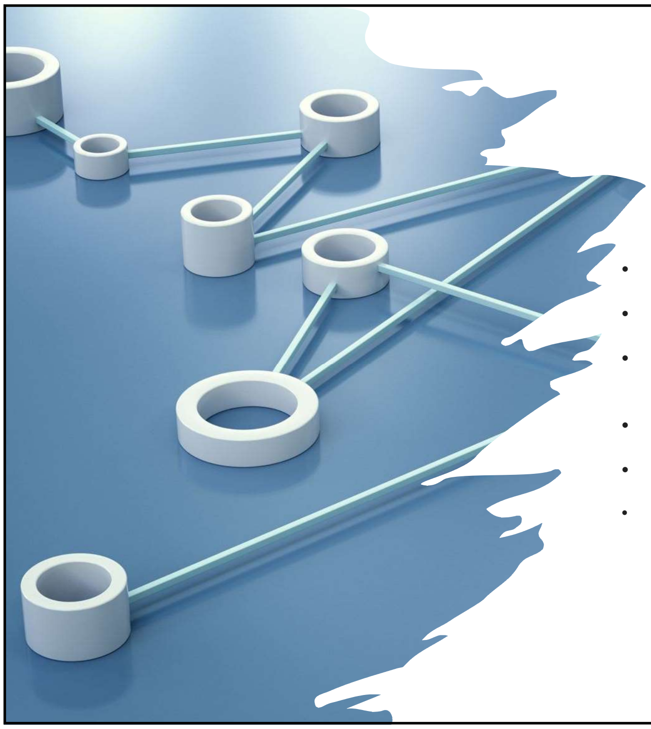
9



Why Now?

- Digital society
- More data
- Need greater processing power to render that data useful

10



Face the Facts

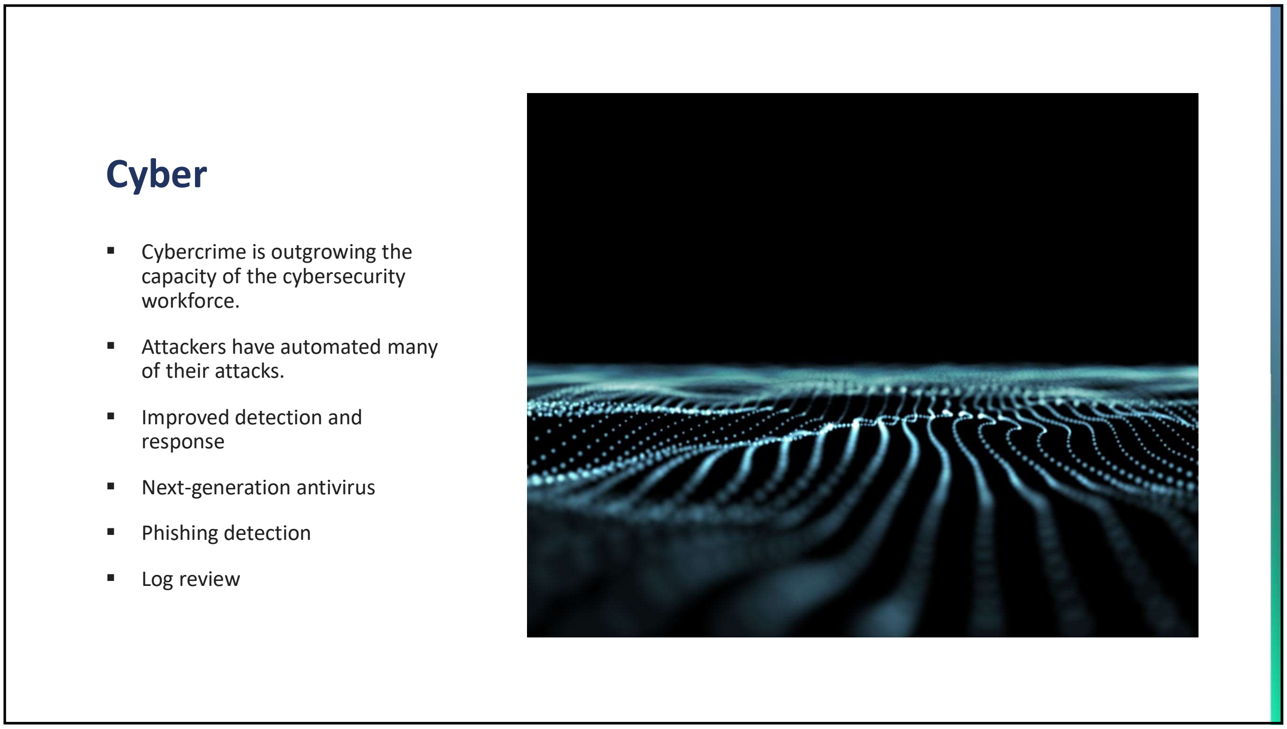
- The global AI market value is expected to reach $267 billion by 2027
- 37% of businesses and organizations already employ AI
- The rise of AI will eliminate 85 million jobs and create 97 million new ones by 2025
- 25 countries are now working on designing autonomous vehicles
- 8 Billion devices use voice assistants (phone, IoT, smart devices, etc.)
- https://dataprot.net/statistics/ai-statistics/#:~:text=Key%20AI%20statistics,billion%20a%20year%20by%202025

11

Examples of AI

- Face ID to unlock a device
- YouTube, Netflix and other recommendation engines
- OpenAI’s ChatGPT. Not a 2023 technology, but a 2023 product.
- ChatGPT made the news because of how accessible it made AI to EVERYONE.

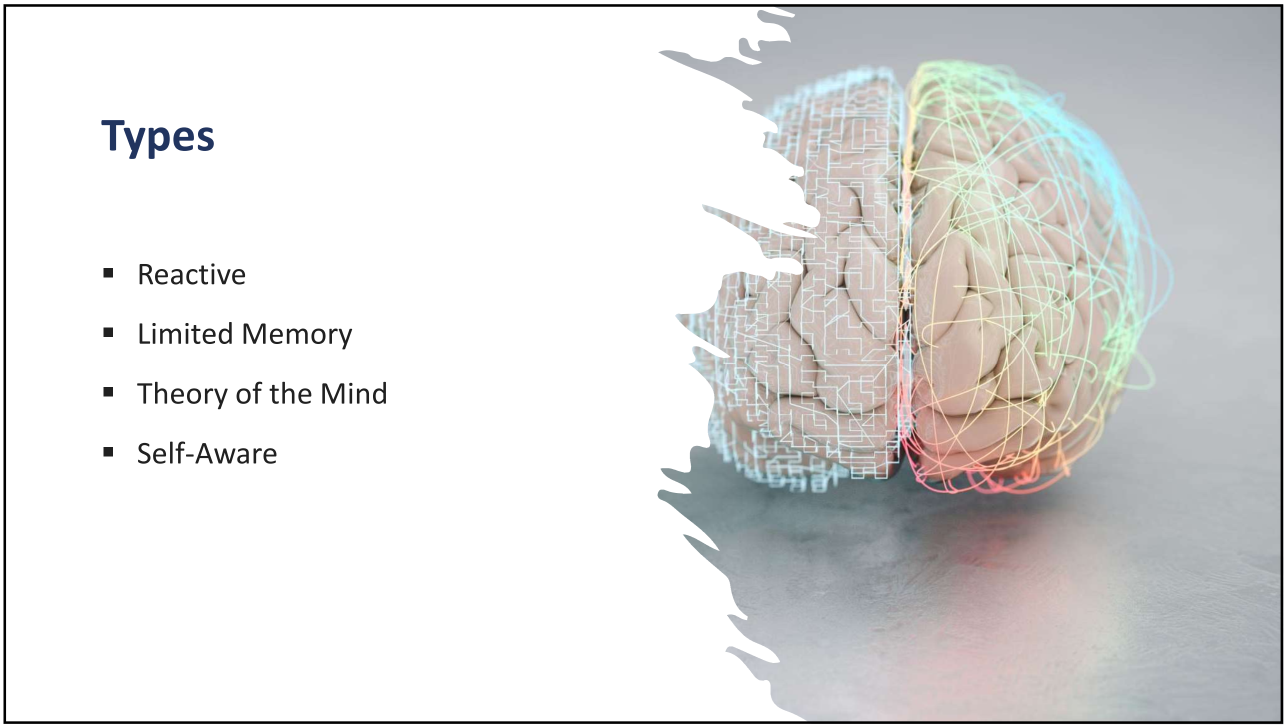
12



Cyber

- Cybercrime is outgrowing the capacity of the cybersecurity workforce.
- Attackers have automated many of their attacks.
- Improved detection and response
- Next-generation antivirus
- Phishing detection
- Log review

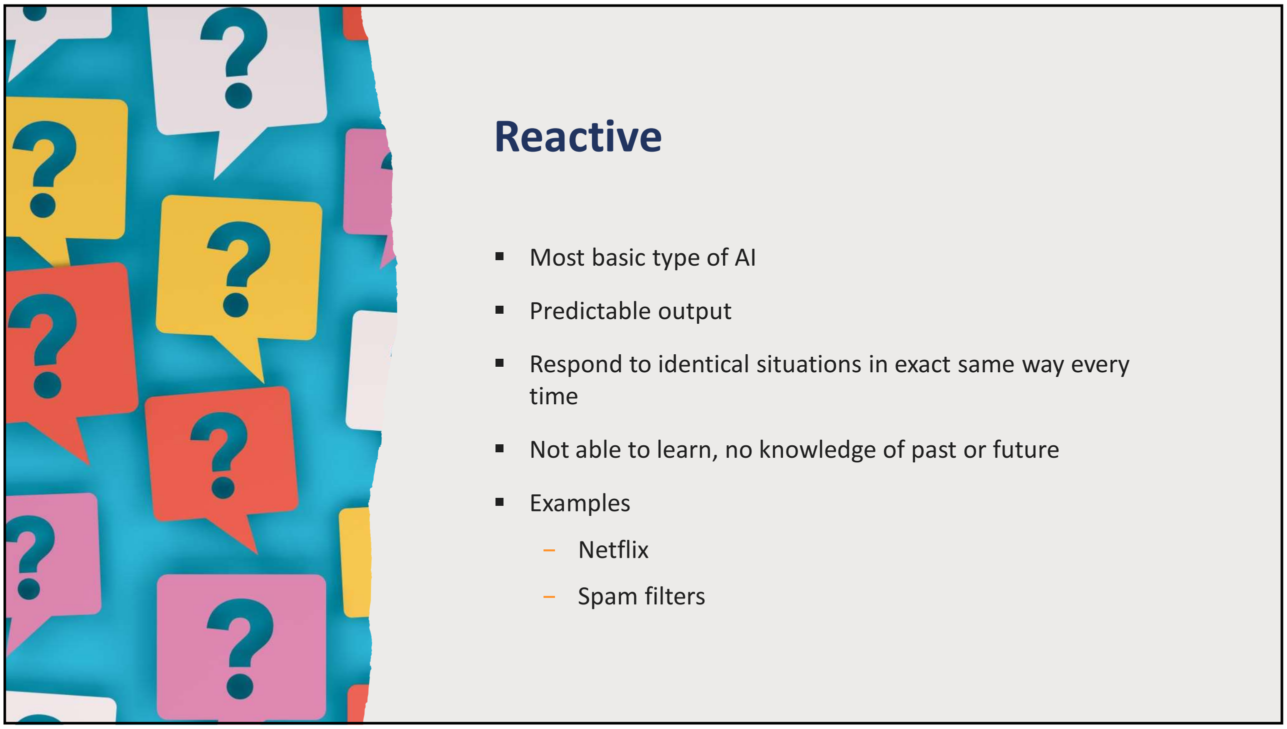
13



Types

- Reactive
- Limited Memory
- Theory of the Mind
- Self-Aware

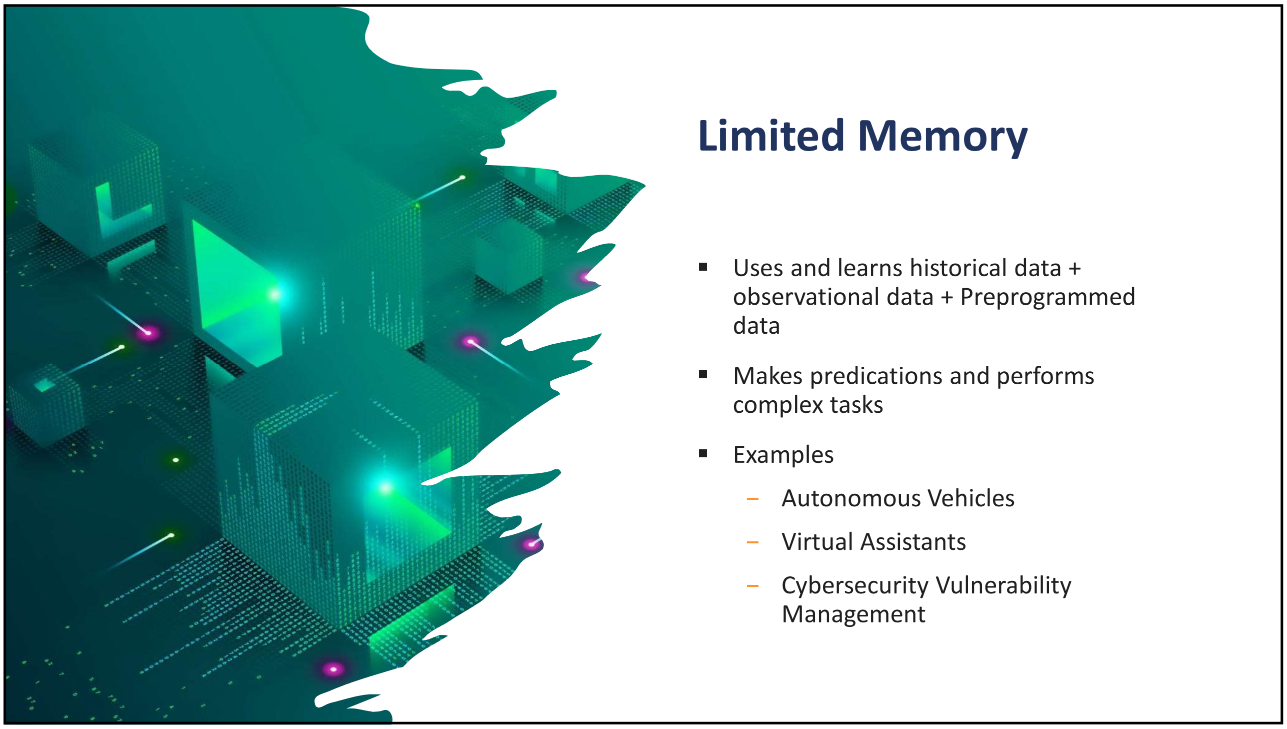
14



Reactive

- Most basic type of AI
- Predictable output
- Respond to identical situations in exact same way every time
- Not able to learn, no knowledge of past or future
- Examples
  - Netflix
  - Spam filters

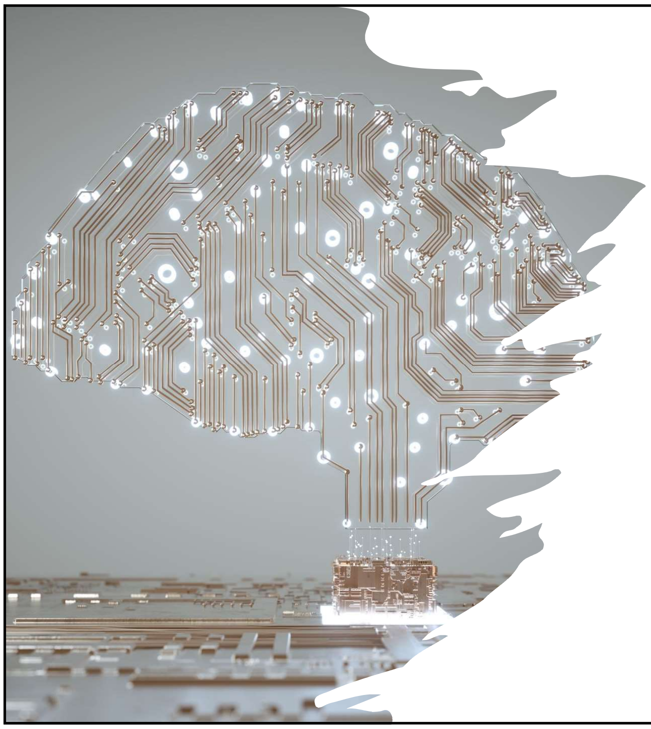
15



Limited Memory

- Uses and learns historical data + observational data + Preprogrammed data
- Makes predications and performs complex tasks
- Examples
  - Autonomous Vehicles
  - Virtual Assistants
  - Cybersecurity Vulnerability Management

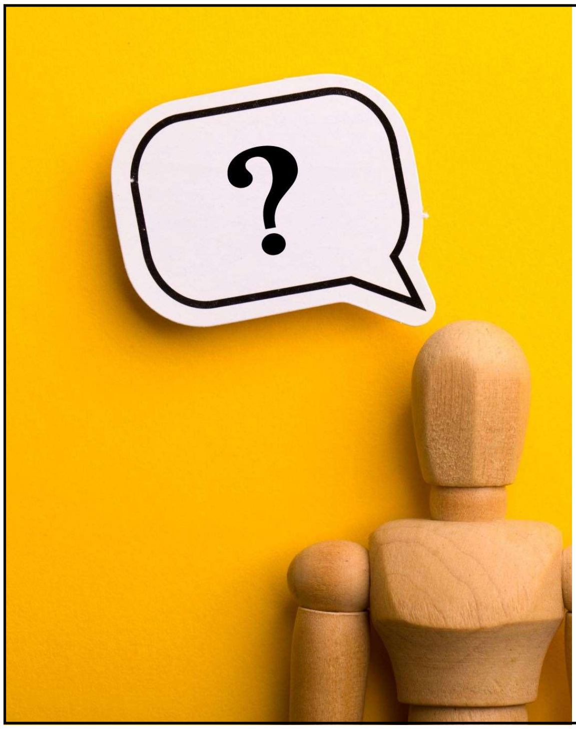
16



Theory of the Mind

- Machine will understand and remember emotions and needs of others
- Complex, emotionally intelligent
- Still under heavy research and development
- Next generation of AI
- Include Artificial Neural Networks (ANNs, an attempt to mimic human brain neural networks)

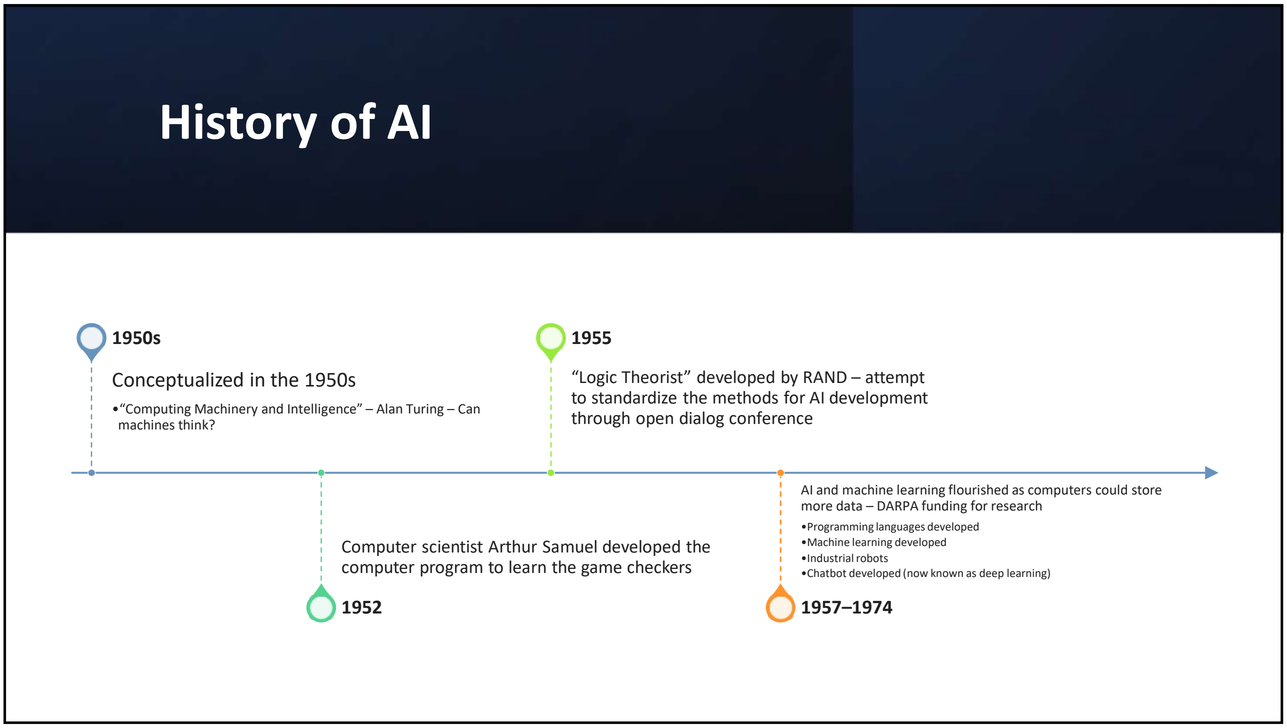
17



Self Aware

- Human like intelligence and self-aware
- Aware of own and others mental states and emotions
- No longer “tools” to be used by humans
- Conscious and feels purpose

18



History of AI

1950s

Conceptualized in the 1950s

- "Computing Machinery and Intelligence" – Alan Turing – Can machines think?

1952

Computer scientist Arthur Samuel developed the computer program to learn the game checkers

1955

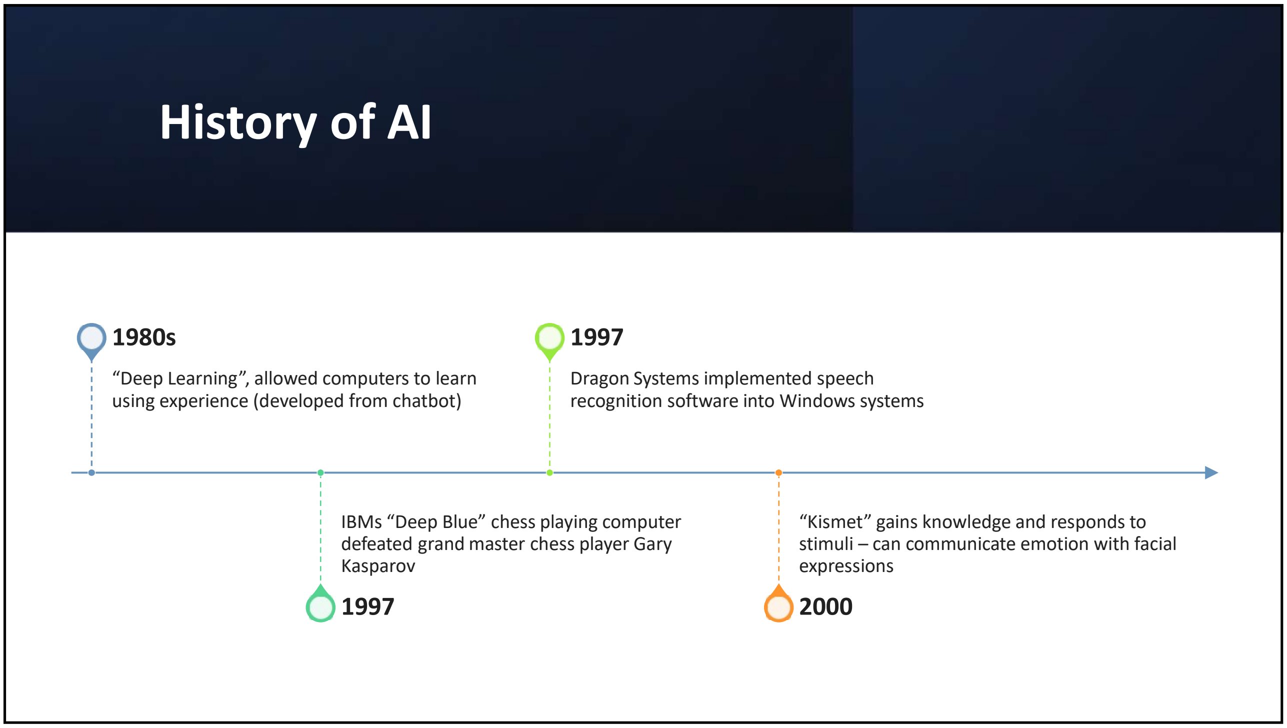
"Logic Theorist" developed by RAND – attempt to standardize the methods for AI development through open dialog conference

1957–1974

AI and machine learning flourished as computers could store more data – DARPA funding for research

- Programming languages developed
- Machine learning developed
- Industrial robots
- Chatbot developed (now known as deep learning)

19



History of AI

1980s

"Deep Learning", allowed computers to learn using experience (developed from chatbot)

1997

IBMs "Deep Blue" chess playing computer defeated grand master chess player Gary Kasparov

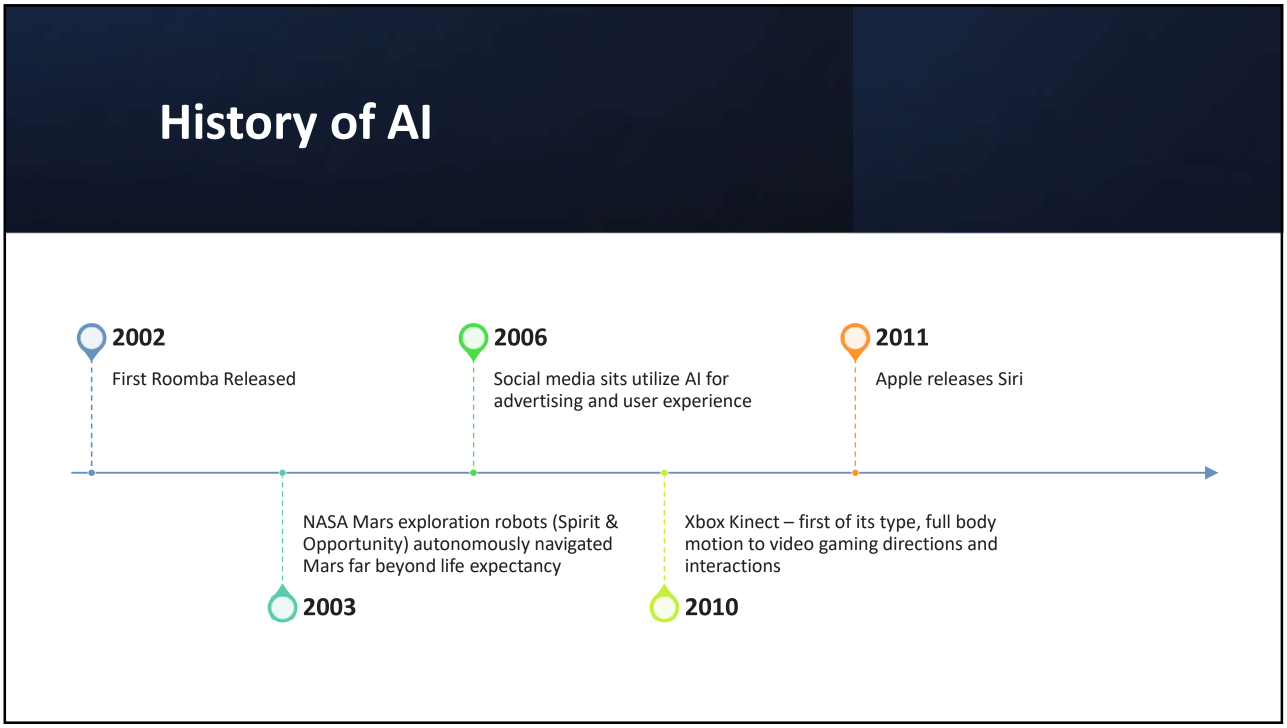
1997

Dragon Systems implemented speech recognition software into Windows systems

2000

"Kismet" gains knowledge and responds to stimuli – can communicate emotion with facial expressions

20



History of AI

2002

First Roomba Released

2003

NASA Mars exploration robots (Spirit & Opportunity) autonomously navigated Mars far beyond life expectancy

2006

Social media sits utilize AI for advertising and user experience

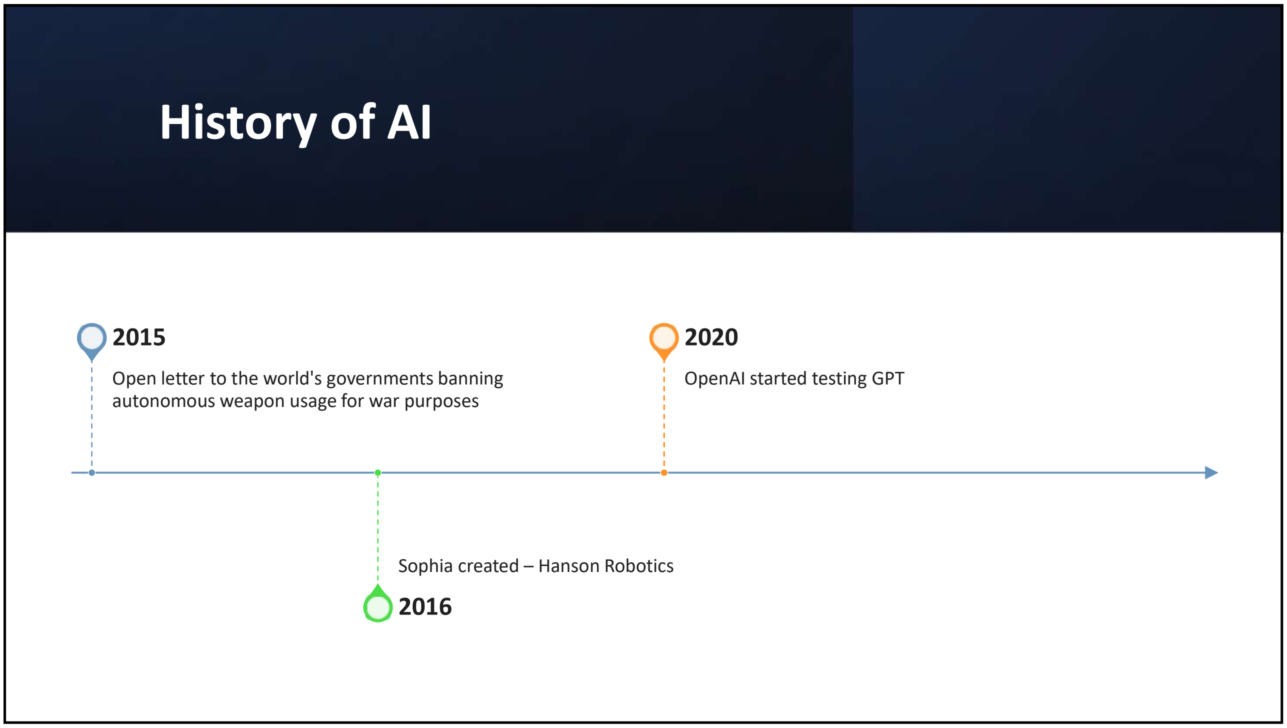
2010

Xbox Kinect – first of its type, full body motion to video gaming directions and interactions

2011

Apple releases Siri

21



History of AI

2015

Open letter to the world's governments banning autonomous weapon usage for war purposes

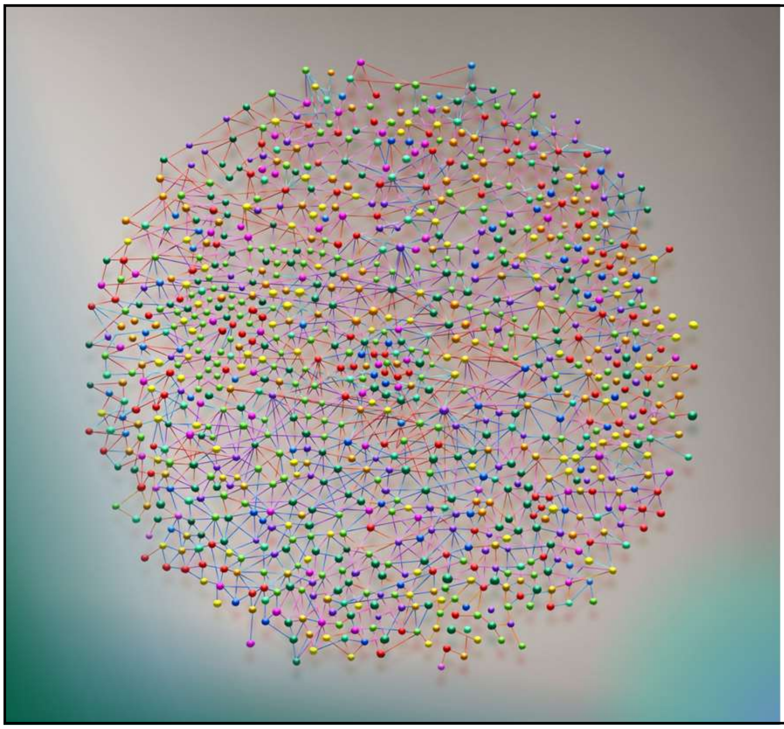
2016

Sophia created – Hanson Robotics

2020

OpenAI started testing GPT

22



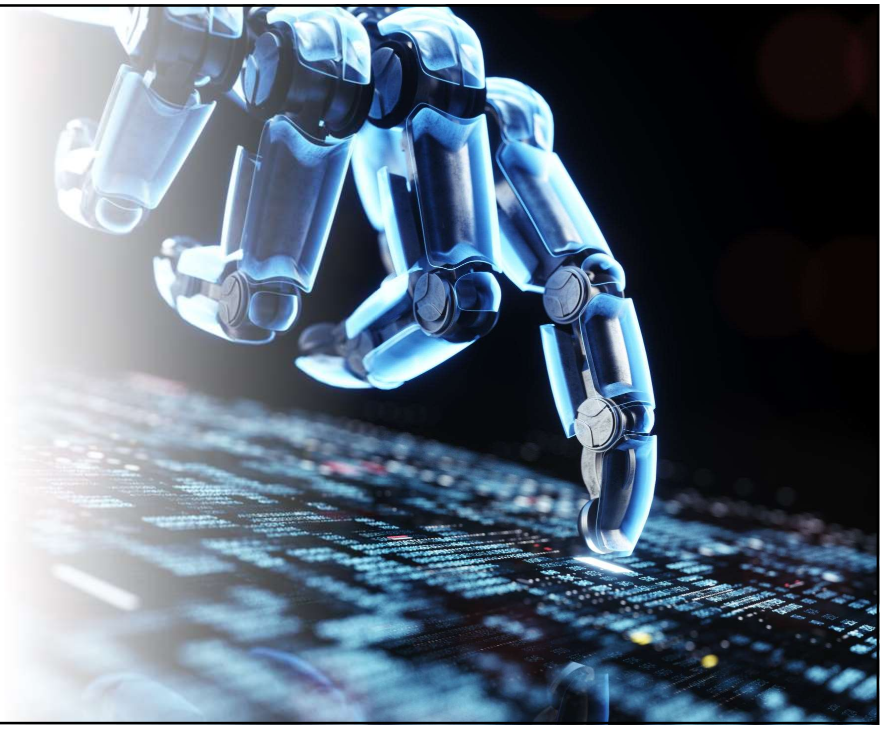
Goals

- Logical Reasoning
- Knowledge Representation
- Planning and Navigation
- Natural Language Processing
- Perception
- Emergent Intelligence

23

Services

- iRobot
- Hanson Robotics
- Softbank Robotics
- Microsoft
- Apple/Google
- Healthcare
- Self-driving cars
- Social media
  - Slack
  - X
  - Meta



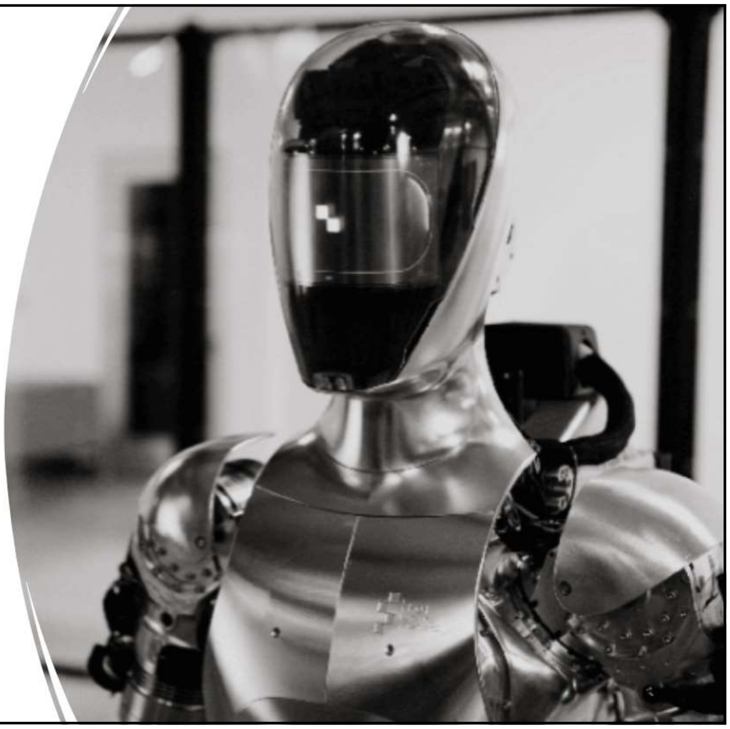
24

Irobot

25

Figure 1

- Figure Status Update - OpenAI Speech-to-Speech Reasoning (youtube.com)



26

Optimus

- Optimus - Gen 2 (youtube.com)

27

Services

- Microsoft
  - Cortana
  - Dynamics 365
  - Bing
  - Microsoft 365
  - Power BI
  - Scheduler
  - Pix

- Azure
- Dynamics 365
- Cognitive Services
- Azure Machine Learning Studio
- Data Science Virtual Machines
- Knowledge Mining
- Conversational AI

28

Social Media

- Instagram/Facebook Meta AI
- xAI
- Snapchat
- Microsoft Teams

29

Language Models

Copilot

Gemini

Supercharge your creativity and productivity

Chat to start writing, planning, learning and more with Google AI

30

Healthcare

Services

31

Self Driving

- Tesla
- General Motors (GM)
- Nuro
- May Mobility
- Cruise
- Waymo
- Aurora

32

Helping Our Astronauts

NASA engineers use A.I. to design spacecraft parts (youtube.com)

33

Defensive Uses

- Threat Detection
- Behavior Analysis
- Vulnerability Management
- Automated Response and Remediation
- User Authentication
- Malware Detection and Prevention:
- Phishing Detection

34

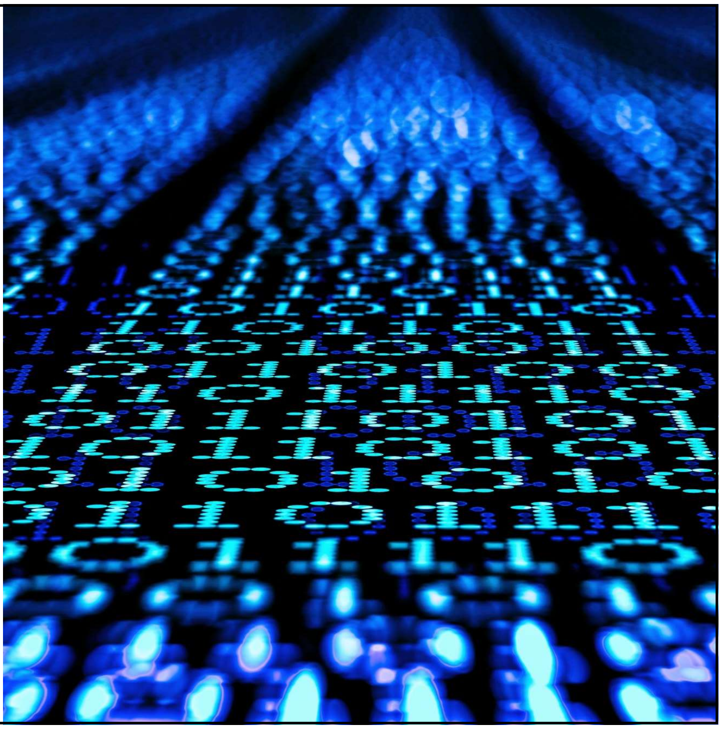
Behavioral Modeling and Generative AI

- Uniform Cost Search (UCS)
- Data-Sets
- Sensory
- Path Planning
- Machine Learning

35

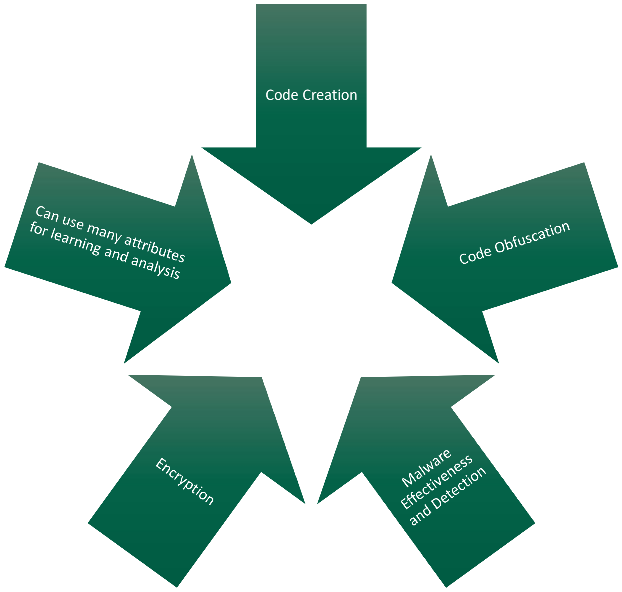
Malicious Uses

- Malware Generation
- Social Engineering
- Deepfakes
- Hacking (exploiting)



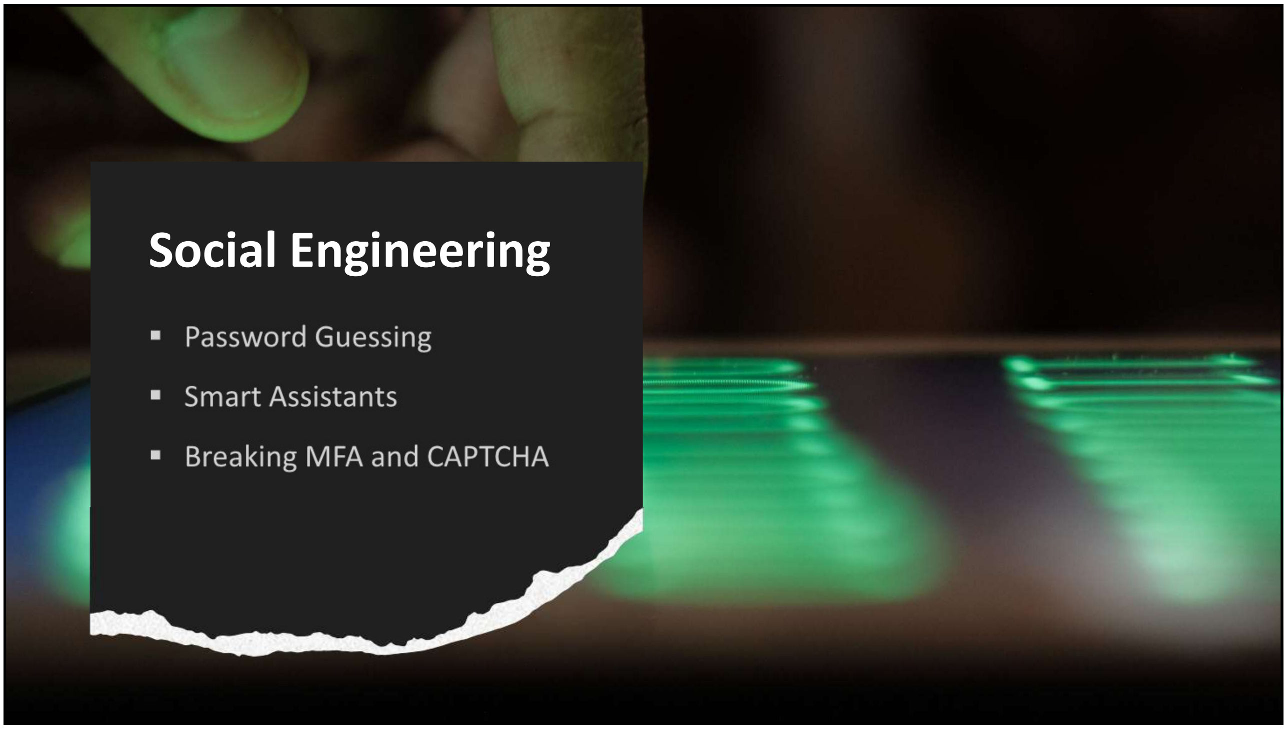
36

Malware Generation



- Code Creation
- Code Obfuscation
- Malware Effectiveness and Detection
- Encryption
- Can use many attributes for learning and analysis

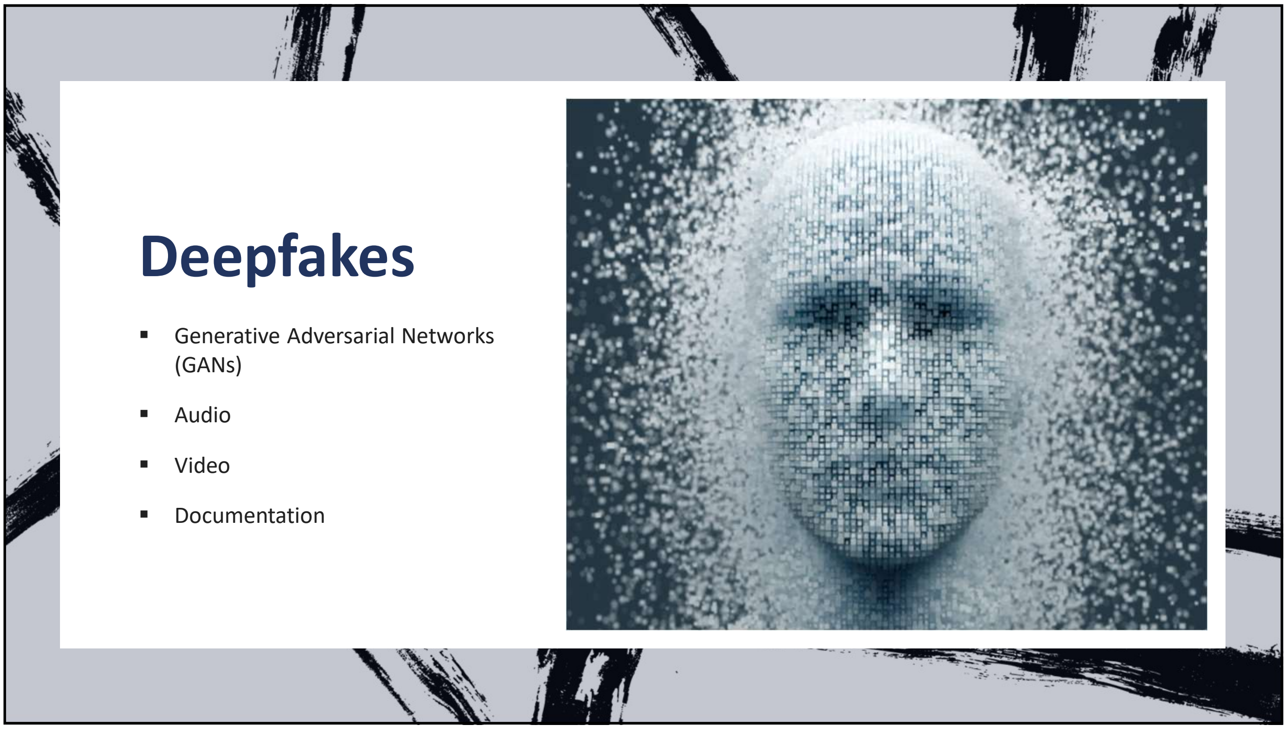
37



Social Engineering

- Password Guessing
- Smart Assistants
- Breaking MFA and CAPTCHA

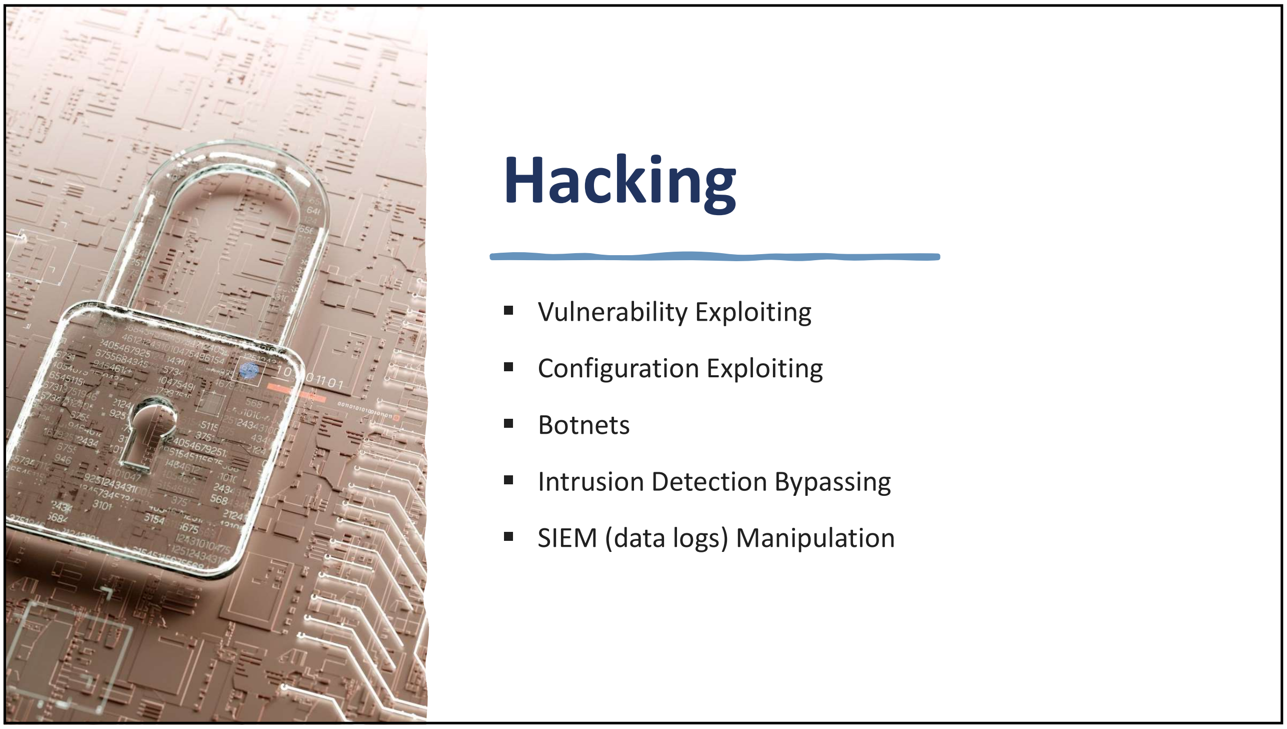
38



Deepfakes

- Generative Adversarial Networks (GANs)
- Audio
- Video
- Documentation

39



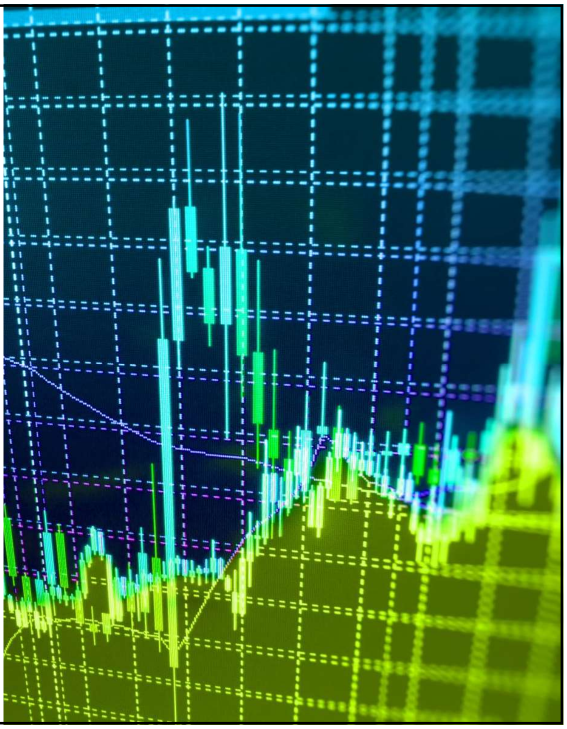
Hacking

- Vulnerability Exploiting
- Configuration Exploiting
- Botnets
- Intrusion Detection Bypassing
- SIEM (data logs) Manipulation

40

Threats to AI

- Data Poisoning
- Data Extraction
- Behavior modification
- Evasion
- Bias/Misuse
- Loss of Control



41

Data Poisoning

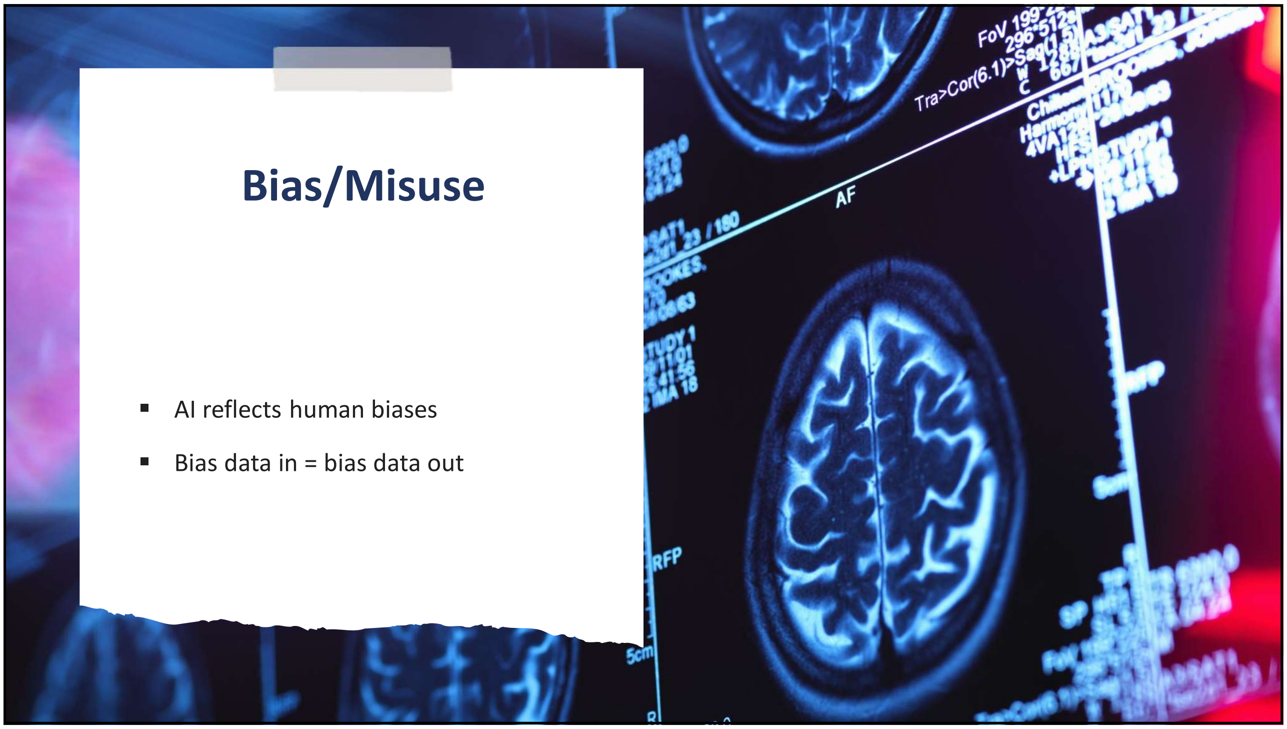
- When Training data is intentionally tampered with
- Affects the results of AI decision making process
- In the form of subtle modifications
  - Label Poisoning – Injecting “mislabeled” or malicious data
  - Training Poisoning – modification of training data
  - Model Inversion – exploiting AI responses to infer information
  - Stealth Attacks – Creating or exploiting known vulnerabilities

42

Data Extraction

- AI is used for
  - Invoicing – Extract key and relevant data
  - Accounting – Financial Statements, expense and revenue reports
  - Tax reporting - Tracking and compiling vast amounts of financial data
  - Pattern Recognition and Extraction

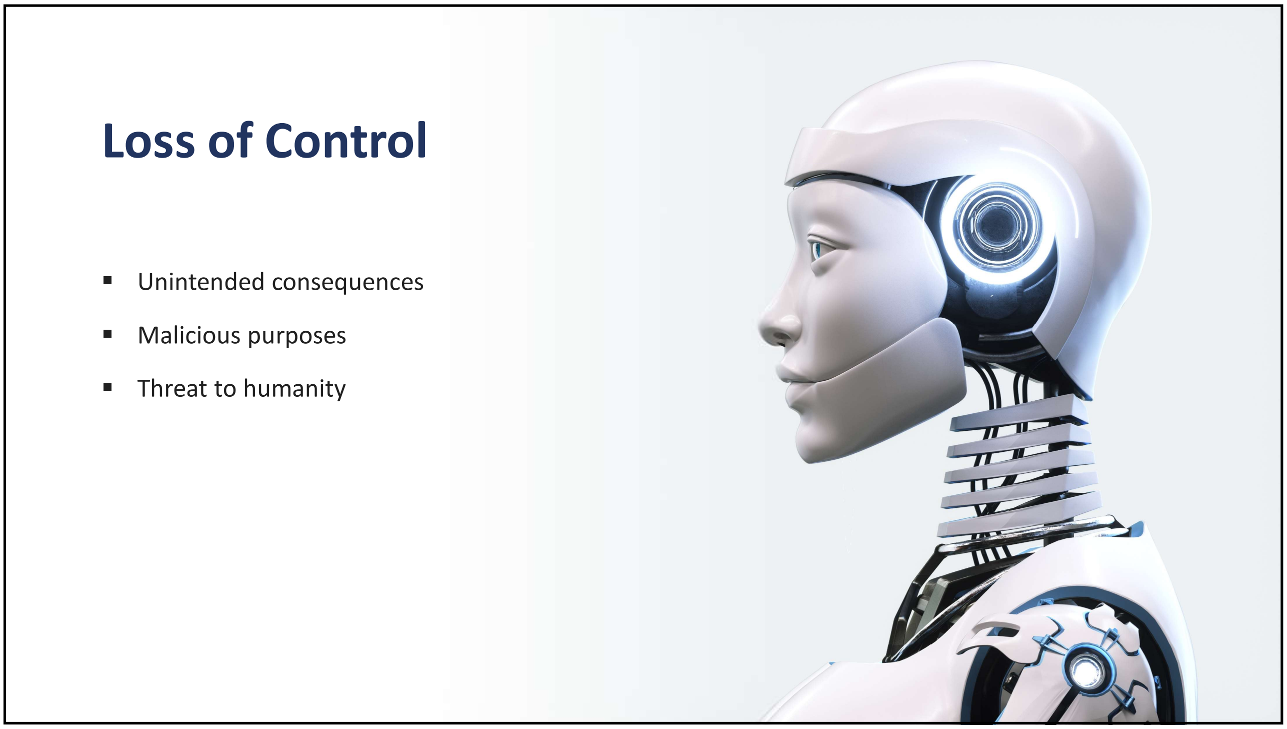
43



Bias/Misuse

- AI reflects human biases
- Bias data in = bias data out

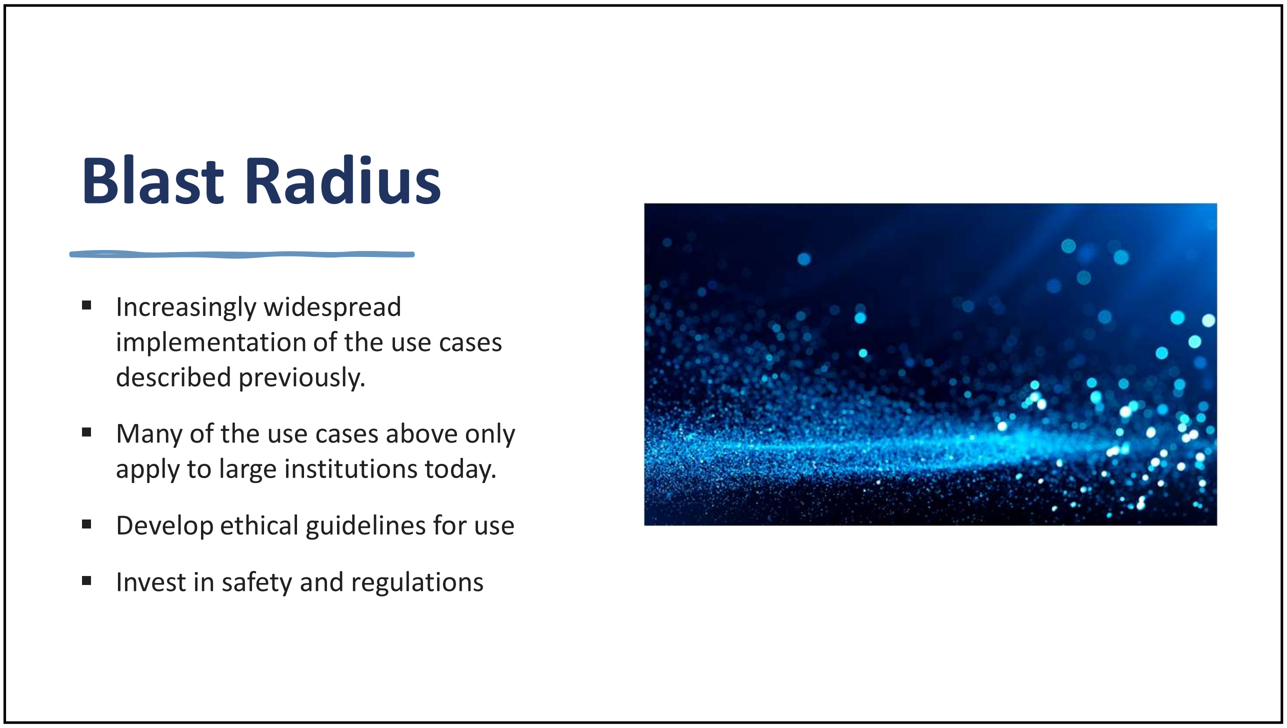
44



Loss of Control

- Unintended consequences
- Malicious purposes
- Threat to humanity

45



Blast Radius

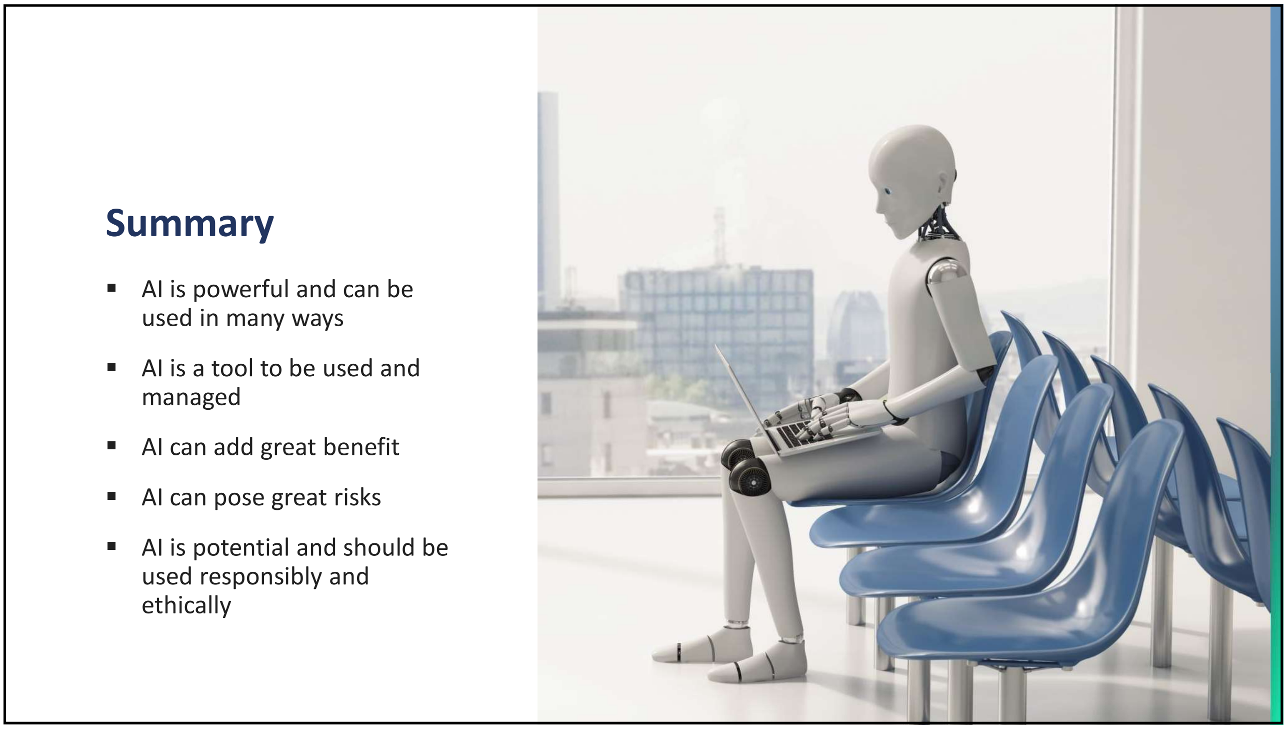
- Increasingly widespread implementation of the use cases described previously.
- Many of the use cases above only apply to large institutions today.
- Develop ethical guidelines for use
- Invest in safety and regulations

46

Will We Be Replaced?

- **No.**
- AI will free up employees to focus on other more complex, customer-facing tasks.
- Many people will still want personal interaction.
- AI can't do everything. Sometimes you need "real" intelligence, not artificial.

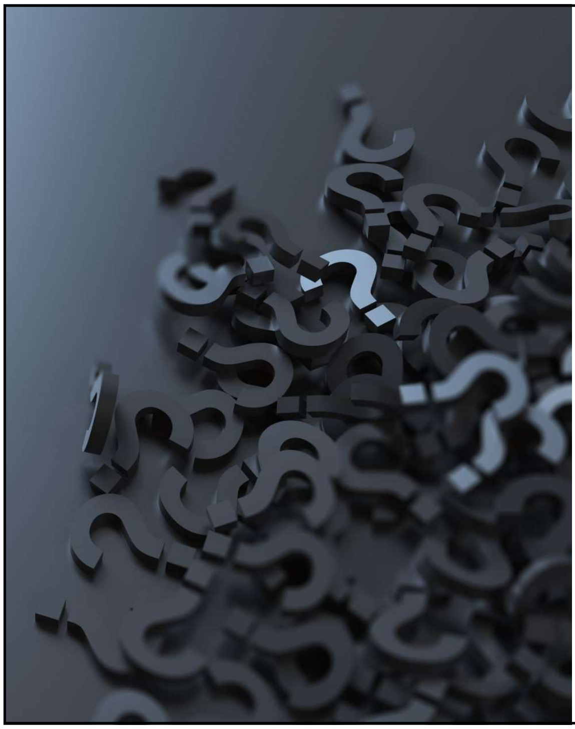
47



Summary

- AI is powerful and can be used in many ways
- AI is a tool to be used and managed
- AI can add great benefit
- AI can pose great risks
- AI is potential and should be used responsibly and ethically

48



Questions?

- Jerad.Glore@vantagepnt.com

49

THANK YOU

VantagePoint
EMPLOYEE OWNED

50