



Panagiotis Kalantzis

Cyber Security & Data Privacy Expert,
CISO, vCISO, Cyber Security Strategist &
Board Advisor

December 2023



Artificial Intelligence in Cyber Security

A Double-Edged Sword



Agenda

01

What is AI

Introduction to History of Artificial Intelligence and Definitions

02

AI and Adversaries

What are the Contributions of AI to Cyber Security Market

03

AI Improvements in CS

What Challenges does AI bring to the Cybersecurity World

04

AI Benefits & Key Takeaways

What Benefits does AI bring to Cybersecurity



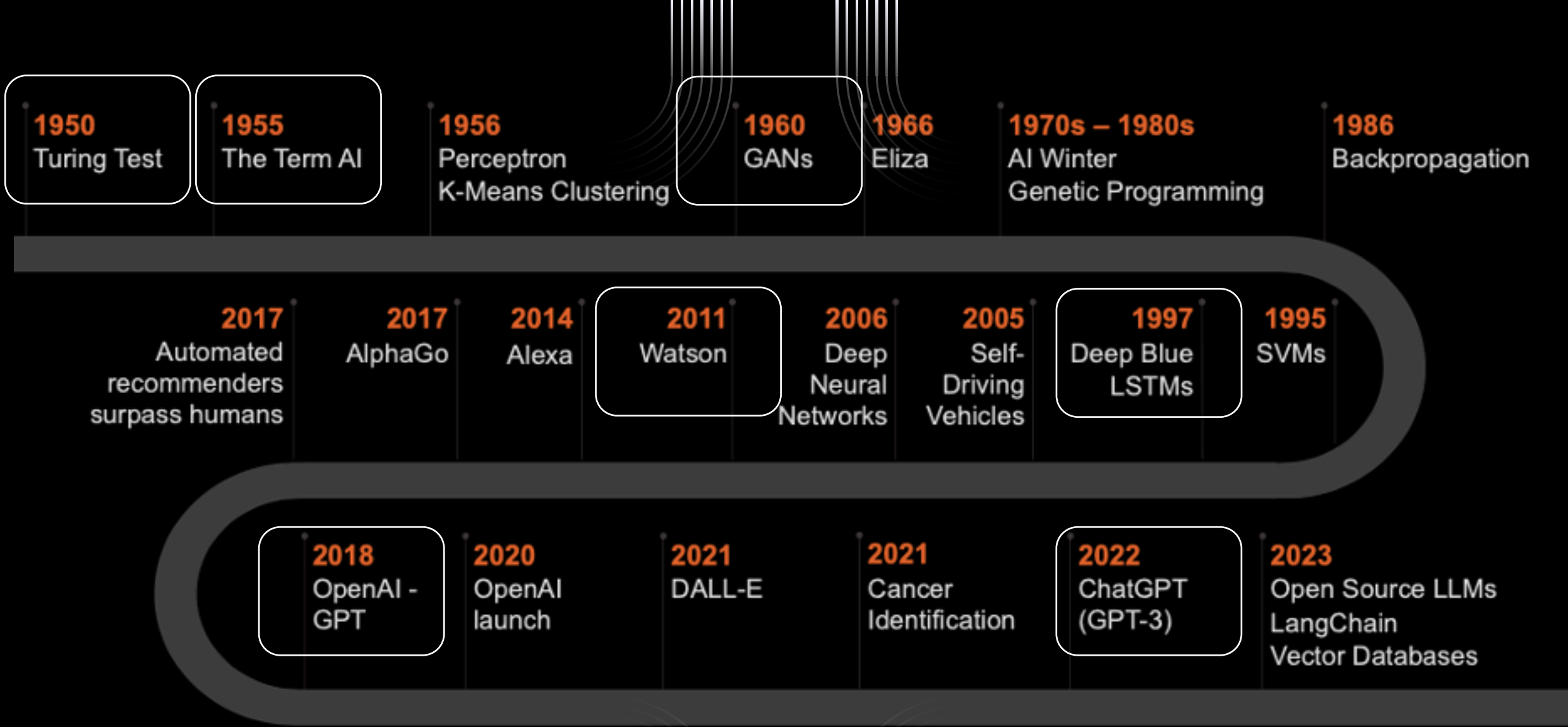
Artificial Intelligence:
Do anything a human would do

AI is Statistics

Careful of the Hype

- Cloud, Blockchain, and now AI ?
- “Cool” products have to have AI

“Everyone calls their stuff ‘machine learning’ or even better ‘artificial intelligence’
- It’s not cool to use statistics!”



Artificial Intelligence is not new

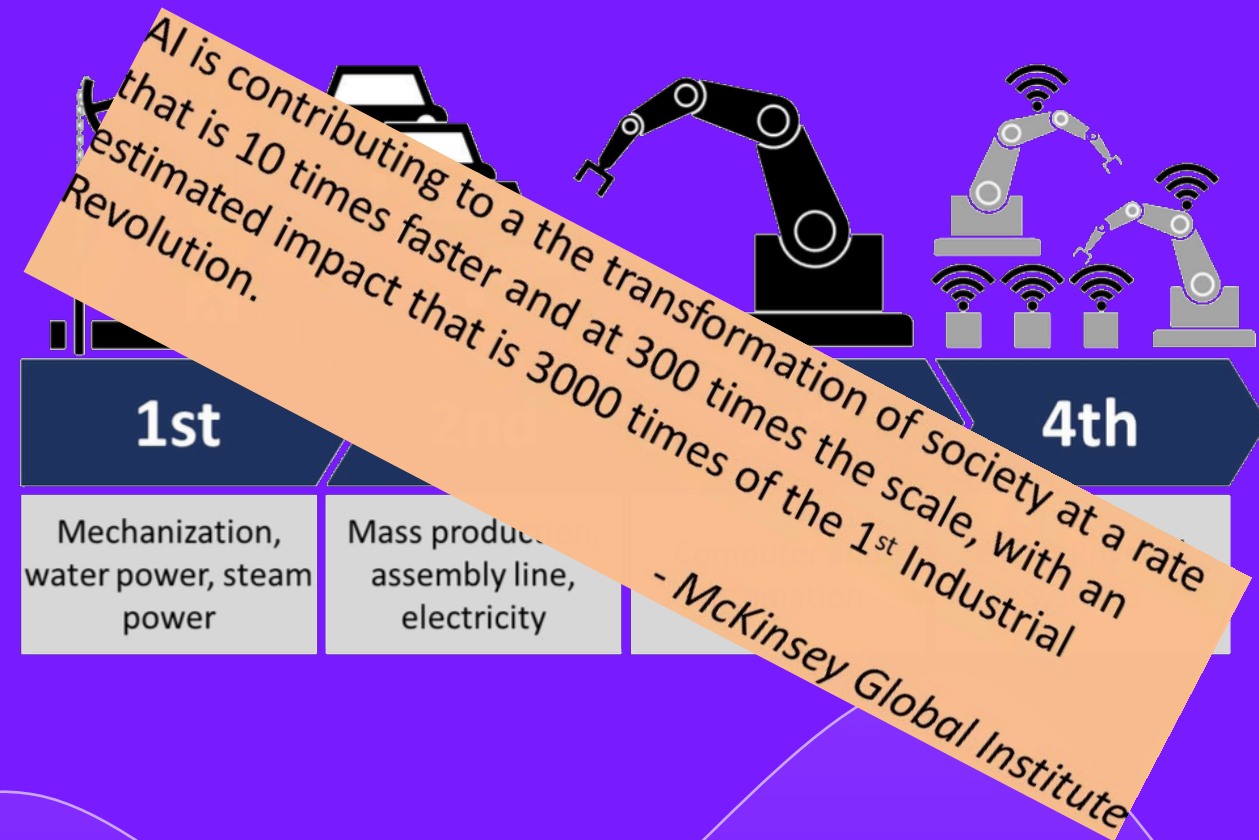
AI & ML leads to Industry 4.0

Industry 4.0 enabled by IoT, Big Data and AI

- IoT is the intelligent sensor
- Big Data will enable processing huge volumes of data
- AI will make sense of the data in decision making

AI helps transform raw data into power - AI will transform businesses for sure

Primarily Machine Learning and then the deeper aspects with Deep Learning



AI is the bedrock on which Industry 4.0 relies on

AI Has Democratized Technology

300 + Application
powered by
GPT+3



Create an app when you've
never coded before



Appeal an insurance denial



Write Excel formulas



Design a personal shopping
assistant



Build new games



Write marketing blogs

For Cyber Security, AI is a Double - Edged Sword



Creates new vulnerabilities that attackers can exploit

Moving at alarming speed, no
reservations



Enhances cyber security

Exercising caution with
deferment to human
expertise



ChatGPT caused observable surge in phishing content (Jan 2023 to Feb 2023)

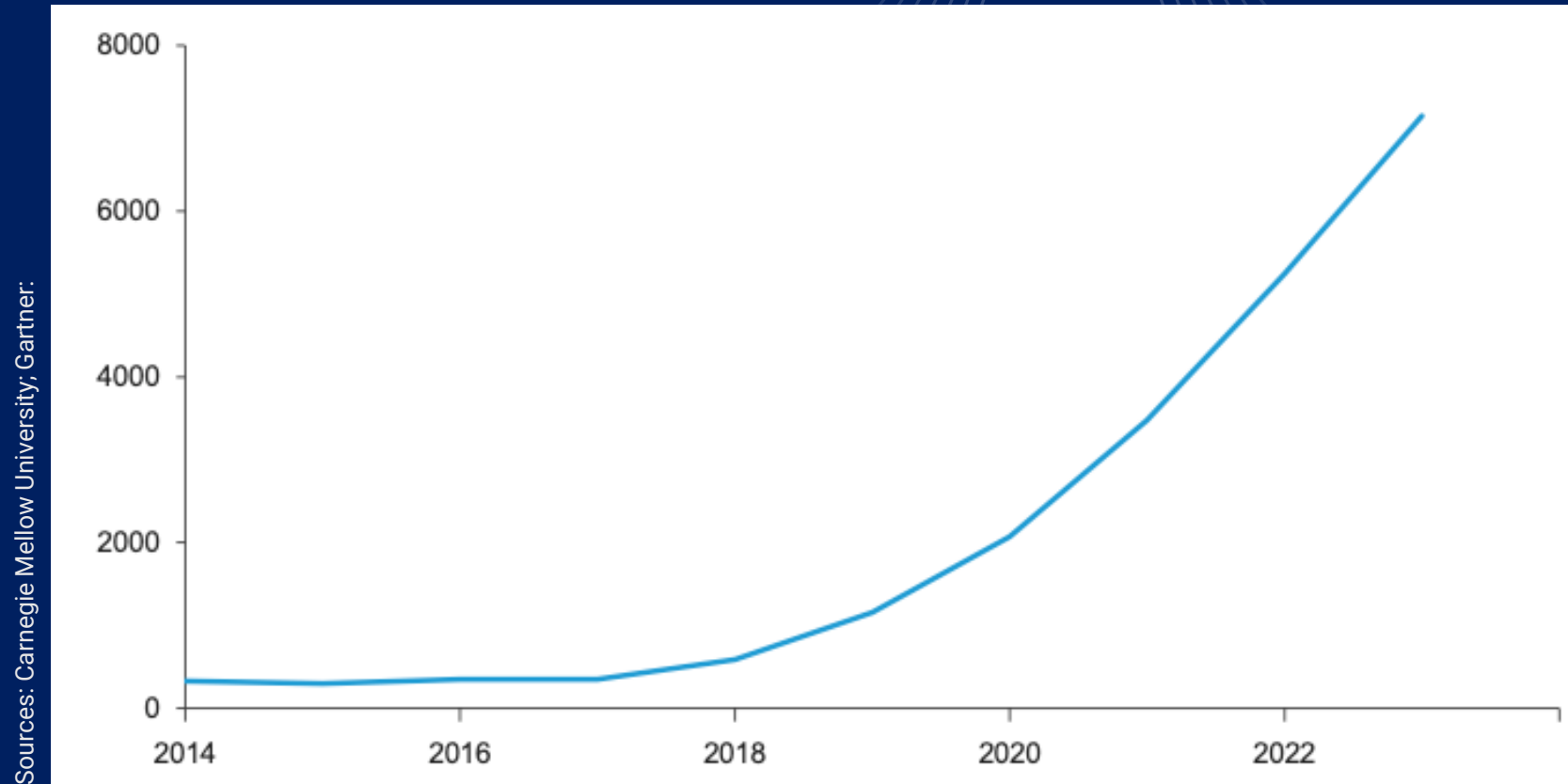


Sophisticated attacks can be created by anyone with ChatGPT account

And it will get worse
BlackBerry's survey of 1,500 IT and cybersecurity decision-makers revealed that 51% of respondents believe a successful cyberattack attributed to ChatGPT will occur within a year

Adversaries Will Increasingly Exploit AI

Number of Pieces of Content Created to Inform Adversarial AI



30% +

A 2021 prediction was that 30% of all cyber attacks were expected to leverage adversarial AI in 2022

Attacks Become more Frequent and Severe

Adversarial AI Can Take many Forms

USING AI TO ATTACK AN ENVIRONMENT

ChatGPT Accelerated Exploit Development

- Increased agility: Vulnerability to code gap closed
- Democratisation: Sophisticated attacks from amateurs
- Attack chain automation: Land and Expand accelerated

Simple Source Code Analysis

- Vulnerability discovery
- Threat surface analysis

AI Augmented Social Engineering

- AI-generated phishing attacks system

ATTACKING A DEFENDER'S AI MODEL

Poisoning Attacks – influencing training data or labels to cause model to underperform

Evasion Attacks – manipulating data during deployment to deceive trained classifiers

Model Extraction Attacks – probing a black box ML system to reconstruct model or extract data it was trained on

Prompt Injection Attacks – injecting malicious data into a prompt directly or via side channels to compromise system

Defenders Must Adapt

- Greater emphasis on efficacy, robust policy creation, and automated response
- Inspection technologies will continue to play a critical and evolving role in security

How Your Adversaries May Attack Your AI



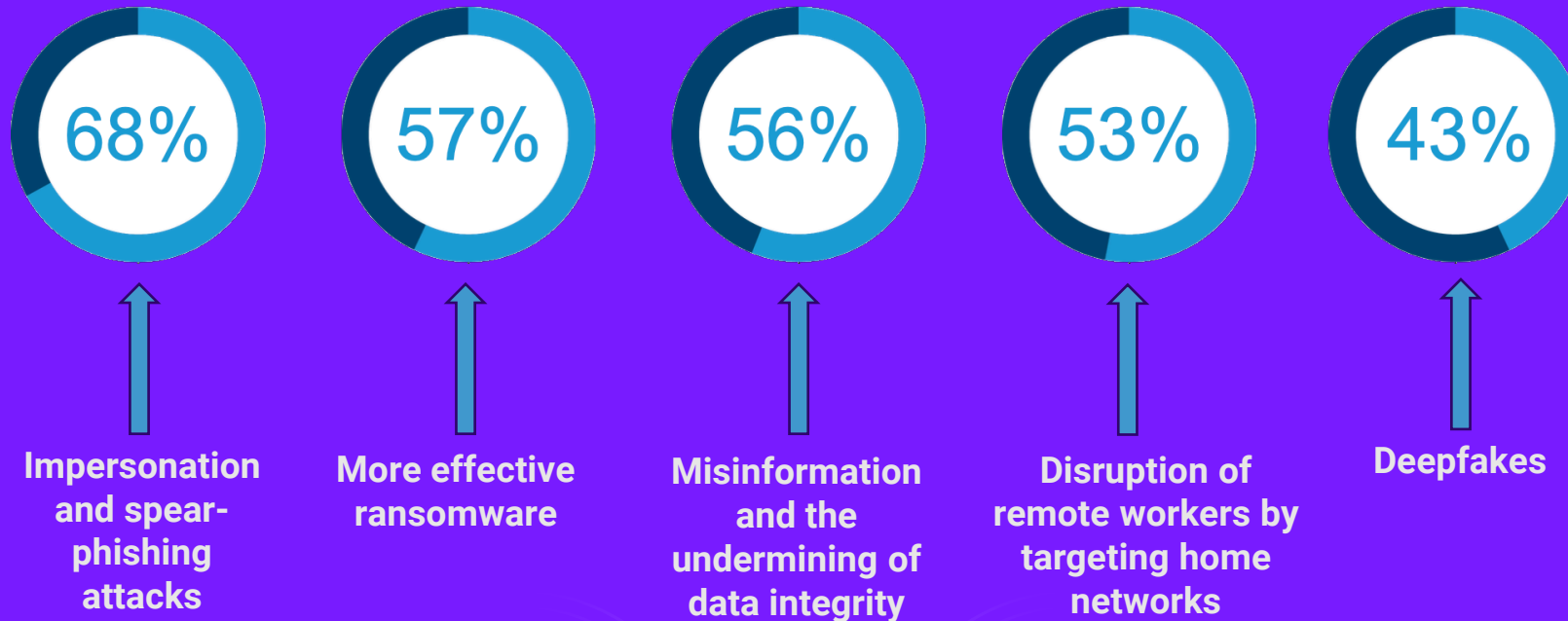
Prompt injection possibilities:

- In downloaded images (steganography, EXIF data, etc.)
- In emails (for LLM based spam filters)
- In common web pages

AI developers focus on rapid feature development and ecosystem expansion, largely ignoring security considerations

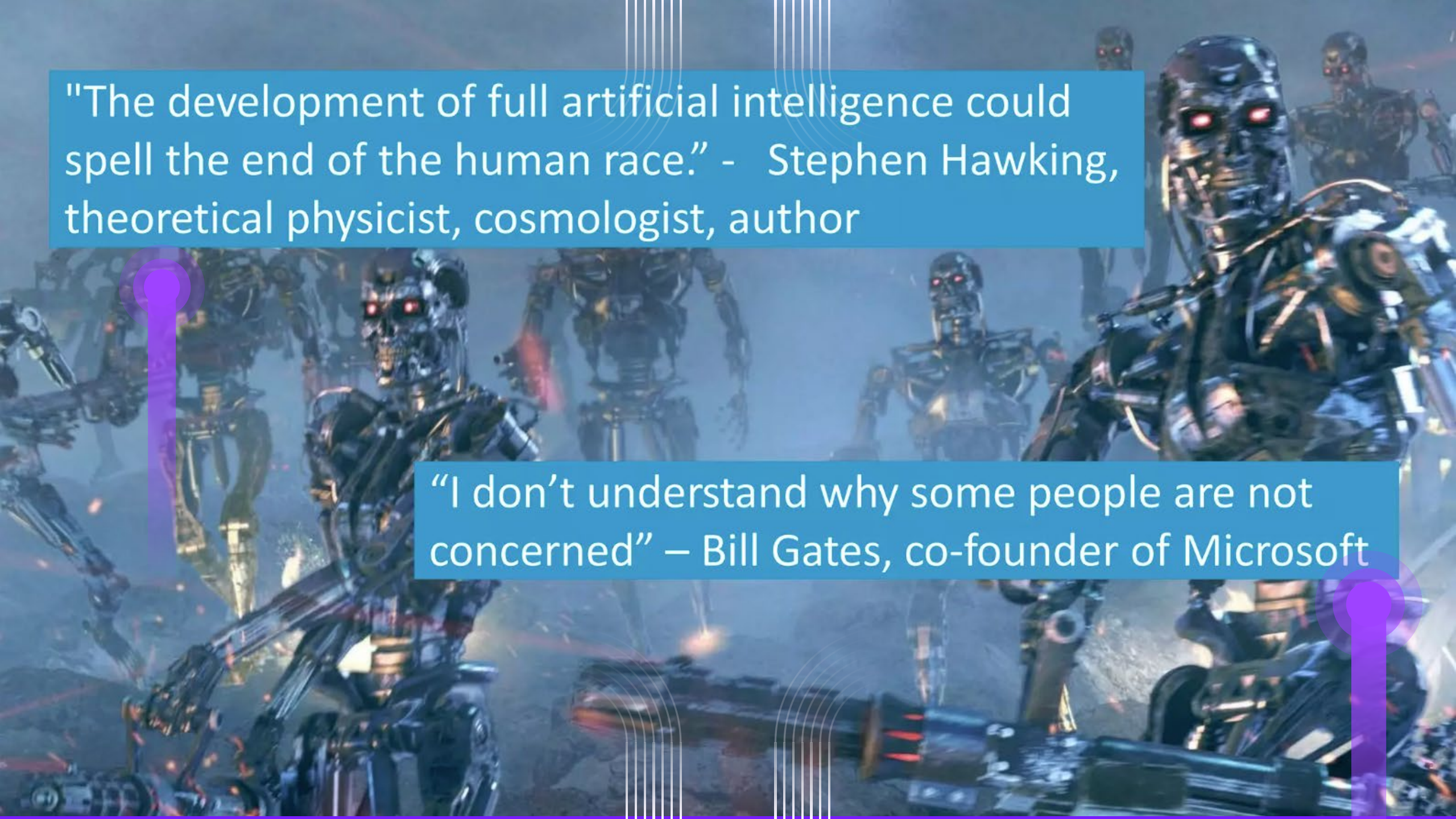
How AI will be used against companies

Impersonate friendly correspondents and launch searing ransomware attacks, execs say



source: MIT Technology Review Insights survey of 309 business leaders worldwide, Jan 2021.

What Can We Expect to See



"The development of full artificial intelligence could spell the end of the human race." - Stephen Hawking, theoretical physicist, cosmologist, author

"I don't understand why some people are not concerned" – Bill Gates, co-founder of Microsoft

AI Advantages in Scale and Speed

Disrupt Security Solutions



Human Domain Knowledge Base

Autogenerated policies based on human-specified goals and constraints



Ingest Data at Immense Scale

Prediction of next attack based on attacker and target profile

Simulation of potential attacks to test and build capabilities



Correlate Massive Data Sets

Automated troubleshooting by correlating across 1000s of events from dozens of sources

Mining big data to find botnets



Faster Detection and Response

Automatic adaptation to environment and continuous app deployment

Smart autoscaling to drive better performance

Ingest Knowledge Beyond Human Scale

Analyze and Respond at Machine Speed

Benefits on Tools based on AI

AI has begun to touch all aspects of cybersecurity

Areas influenced:

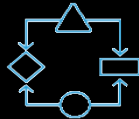
- Malware Detection
- Intrusion Detection / Prevention
- Antispam
- Vulnerability Management
- Social engineering
- Data Classification
- Threat Intelligence
- Penetration testing
- Data security



Where We Are

- Sophisticated point protections
- Nascent AI/ML capabilities
- Rapidly changing attack surfaces

Challenges



Product **design process doesn't embrace use of big data** for efficacy and ease of use



Isolated thinking about big-picture strategy, and **no urgency** to move fast together

Opportunities



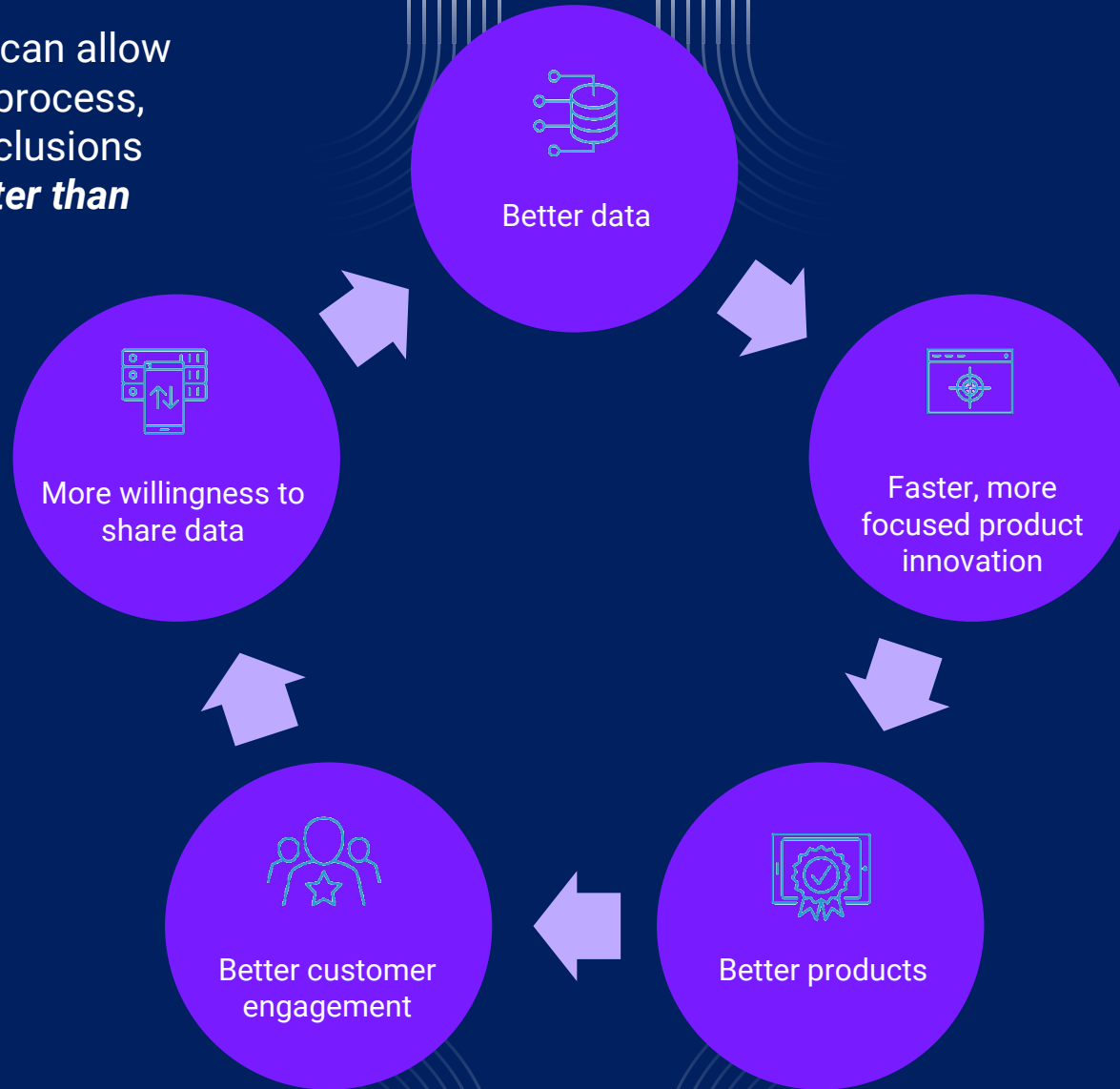
Cross-silo data stores, analysis tools, visualisations, and ingestible events



Easy-to-use / add ability to send and land operational telemetry across all security tools

The Cyber Security Industry's AI Undertaking

Generative AI can allow us to absorb, process, and draw conclusions from data **faster than ever before**



... but to be fully realised, we require cyber security products to be **more inter-connected into the cycle** than they've ever been

The Virtuous Cycle of Data

AI as a Savior



Arms Race of Offensive & Defensive Use of GenAI

Security Copilot

Purple AI

Sec-PaLM

Charlotte AI

PentestGPT

PassGPT

FraudGPT

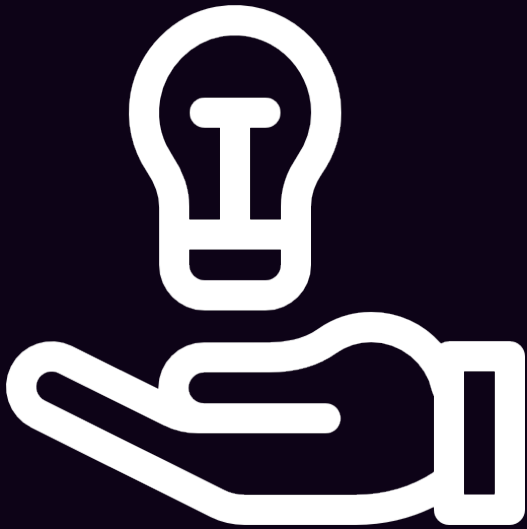
WormGPT

Gartner



Plenty of New Cyber
Security Jobs

Key Takeaways



Embrace what is happening here

There is nothing to fear about Artificial Intelligence, but security professionals must be clear-eyed about the threat surface

The sword has two edges

Adversaries have equal access to the same AI tools that you have

AI systems benefit most from sharing

Data isolation of cyber security information eliminates potential

Some words about me

- ~ 25 years in the field of Information Security and Cybersecurity
- Extensive domestic and international experience in Information Security, Data Protection and Risk Management Consulting
- Passionate about embedding risk into IT and business cultures and aligning information security and data protection needs with broader business goals
- Speaker at numerous events and Author
- Master's degree in Information Systems from the Athens University of Economics and Business
- Degree in Mathematics from the University of Patras.
- Professional certifications from recognized institutions such as ISC2, ISACA and IRCA, as well as leading technology suppliers.



Panagiotis Kalantzis

Cyber Security & Data Privacy Expert,
CISO, vCISO, Cyber Security Strategist &
Board Advisor



in [linkedin.com/in/pkalantzis](https://www.linkedin.com/in/pkalantzis)

 [kalantzis.me](https://www.kalantzis.me)

 pkalantzis@gmail.com