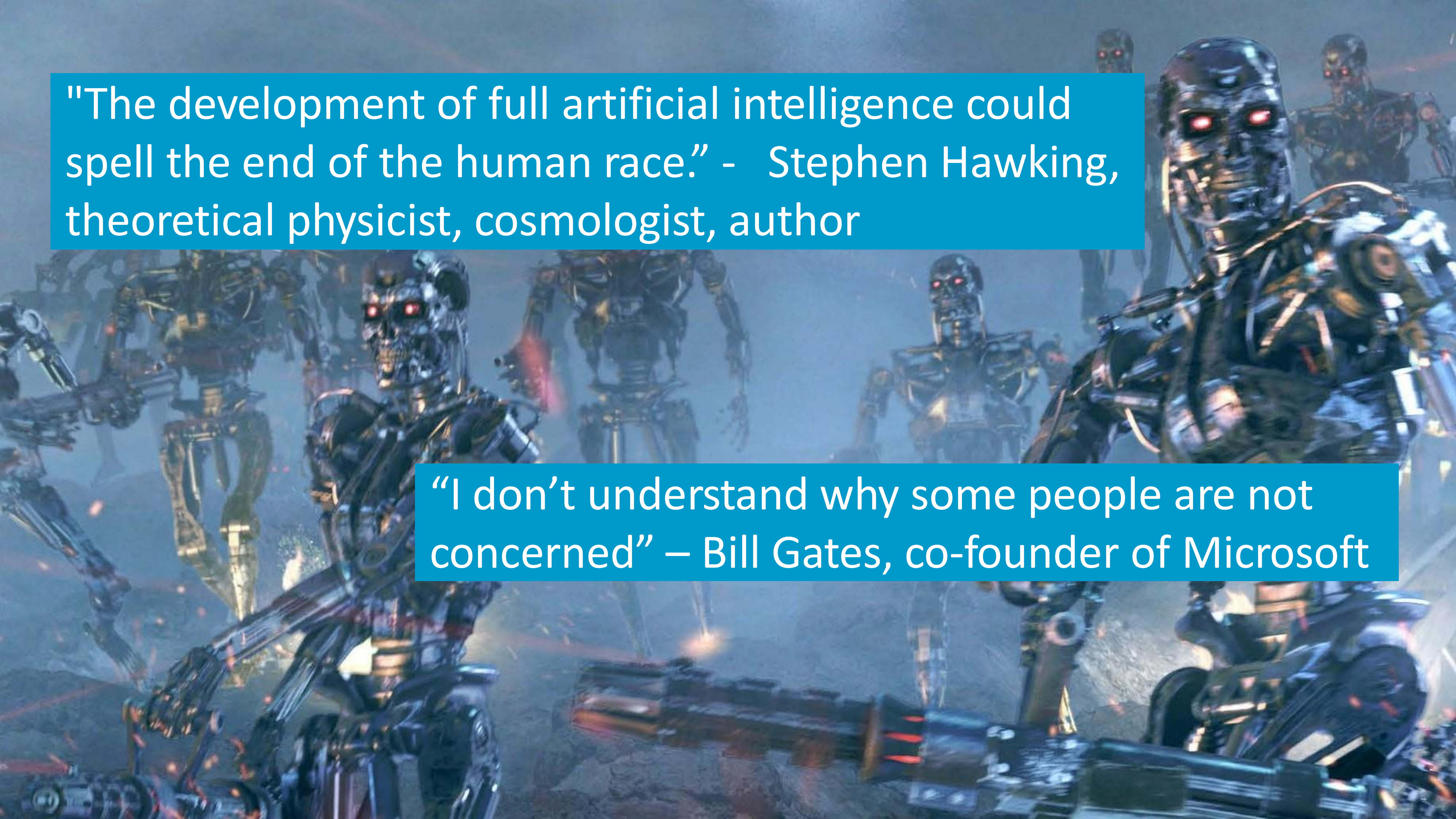
Combating Cybersecurity

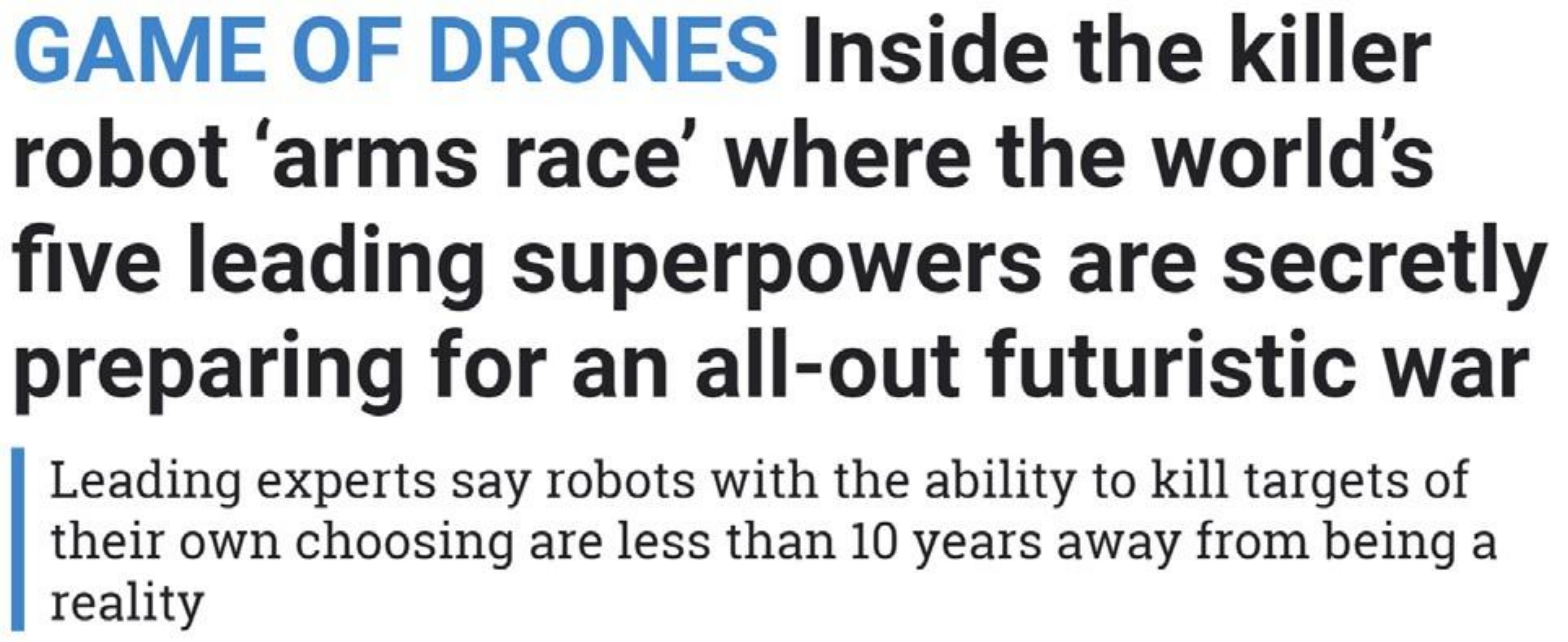
Threats with AI and Machine Learning

Col Inderjeet Singh
CIO , Vara United Ltd



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

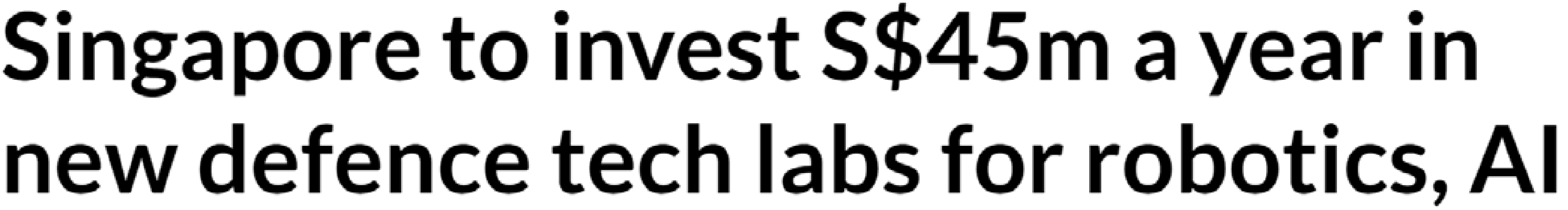
“I don’t understand why some people are not concerned” – Bill Gates, co-founder of Microsoft



GAME OF DRONES Inside the killer robot 'arms race' where the world's five leading superpowers are secretly preparing for an all-out futuristic war

> Leading experts say robots with the ability to kill targets of their own choosing are less than 10 years away from being a reality

Kalashnikovs of tomorrow



Singapore to invest S$45m a year in new defence tech labs for robotics, AI

Man or Machine? Advanced Behavioral Attacks

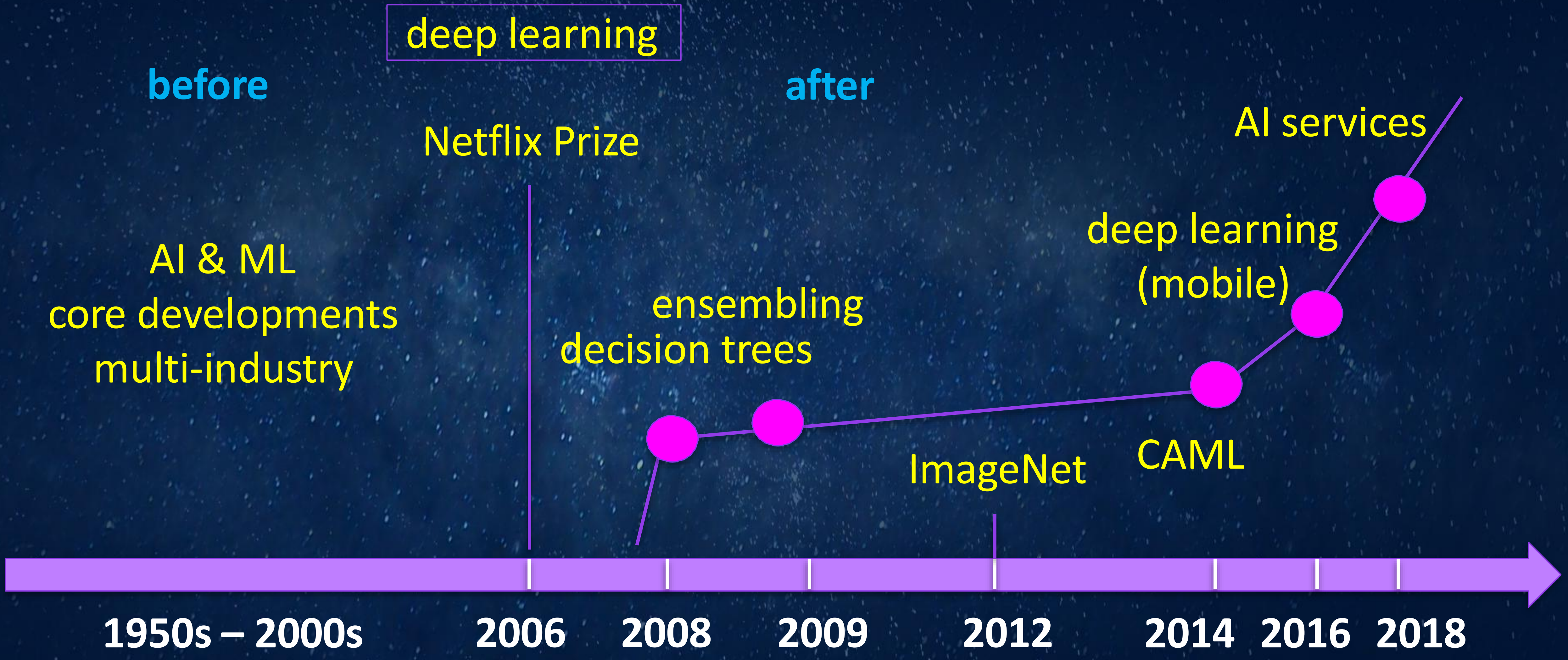
- Imagine a business email compromise attack
  - you get an email to wire payment for an invoice from the CFO
- The email is written from your CFO
  - natural language processing from emails
- You're suspicious and call the CFO
- But your phone is compromised
- You're connected to adversary who has a speechbot with your CFO's Voice
- Science fiction or possible today?

Microsoft Real-Time Translation (2012)

I'm speaking in english and hopefully you'll hear me speaking chinese in my own voice.
Again, the results are not perfect.
They are in fact quite a few errors.
我是说英语，希望你能听我说中国人自己的声音。
再次，结果并不完美。
他们实际上不少错误。

https://www.youtube.com/watch?v=Nu-nlQqFCKg

Is AI/ML New? No*



deep learning

before

after

Netflix Prize

AI services

AI & ML
core developments
multi-industry

deep learning
(mobile)

ensembling
decision trees

ImageNet

CAML

1950s – 2000s

2006

2008

2009

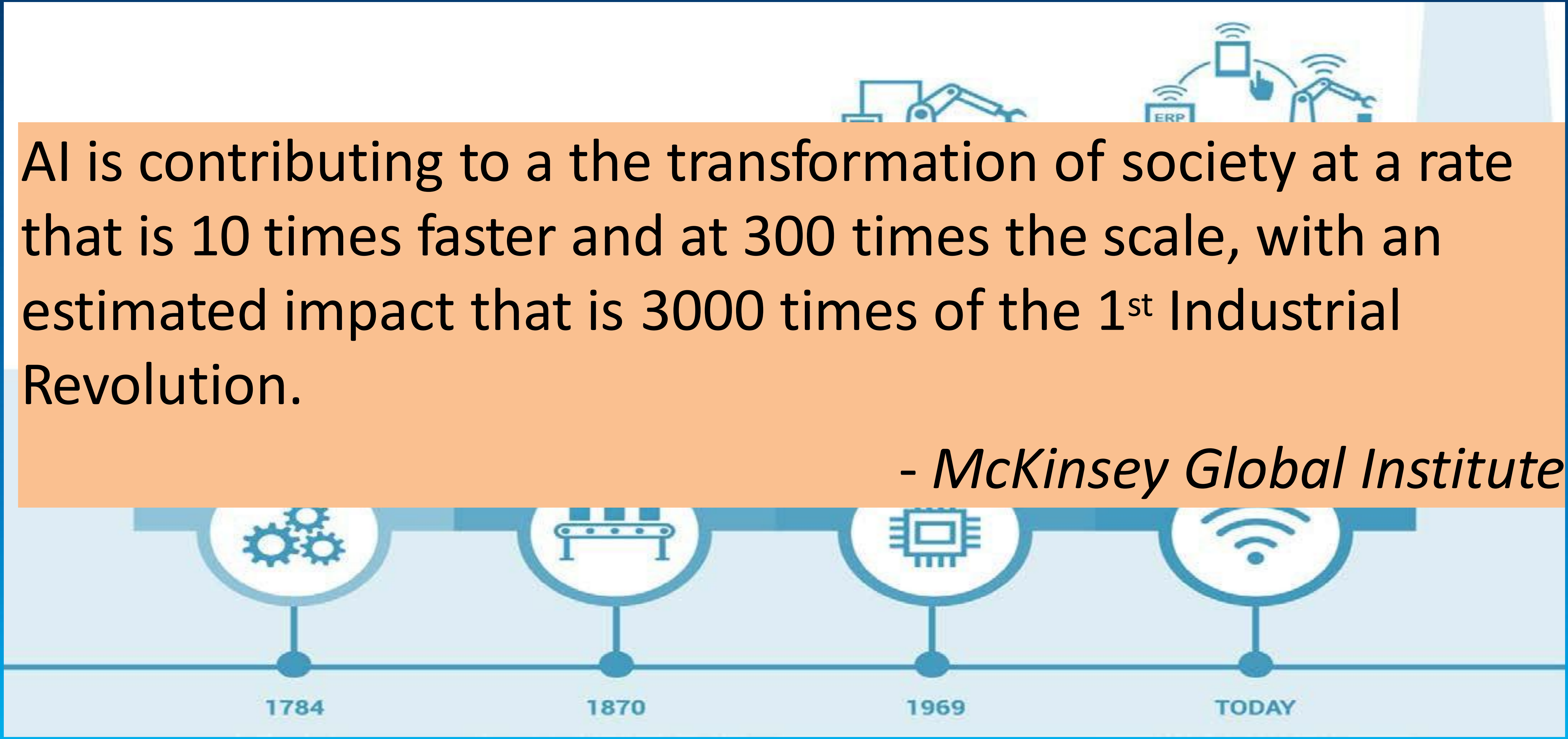
2012

2014

2016

2018

Fourth Industrial Revolution

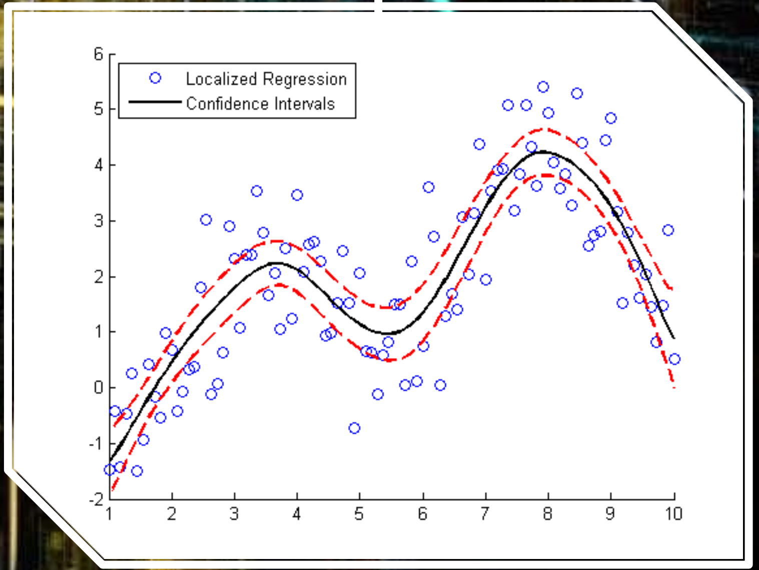


AI is contributing to a the transformation of society at a rate that is 10 times faster and at 300 times the scale, with an estimated impact that is 3000 times of the 1st Industrial Revolution.

- *McKinsey Global Institute*

Artificial Intelligence

Robotic Process Automation



Machine Learning Algorithms

Applications of Artificial Intelligence

Healthcare

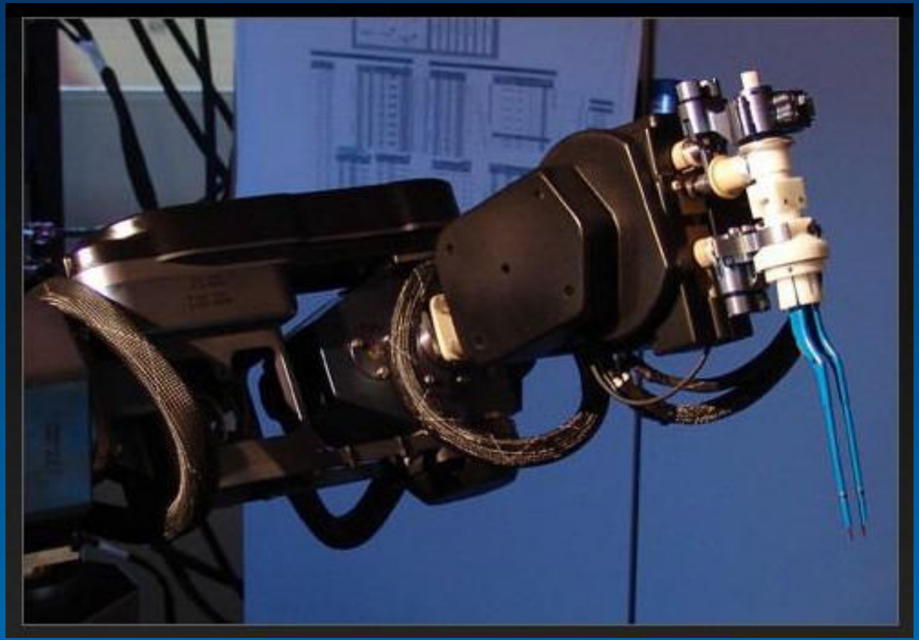
Accounting & Law

Cyber Security

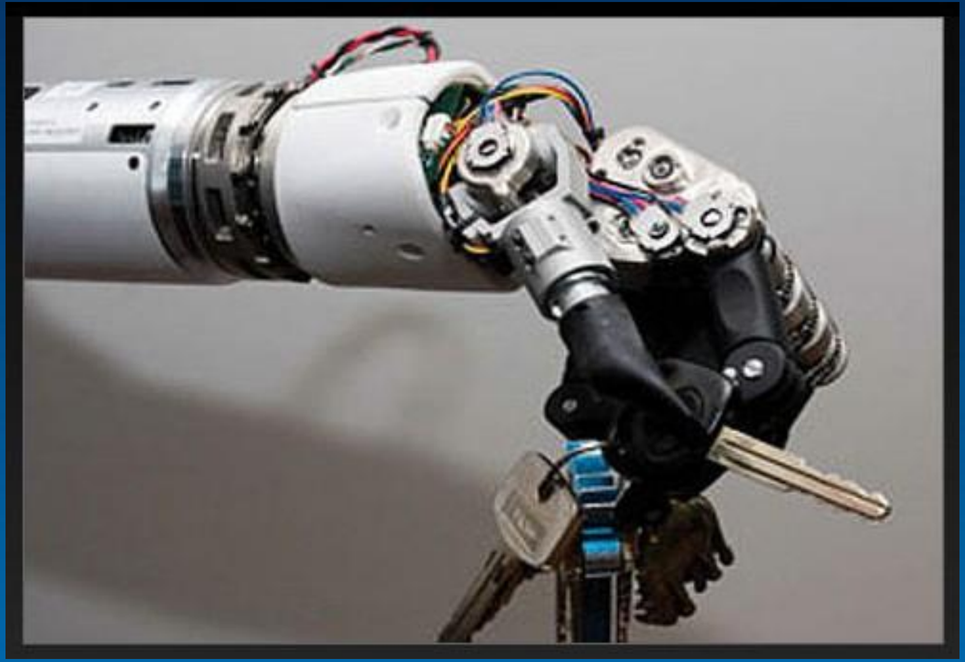
Military

Finance

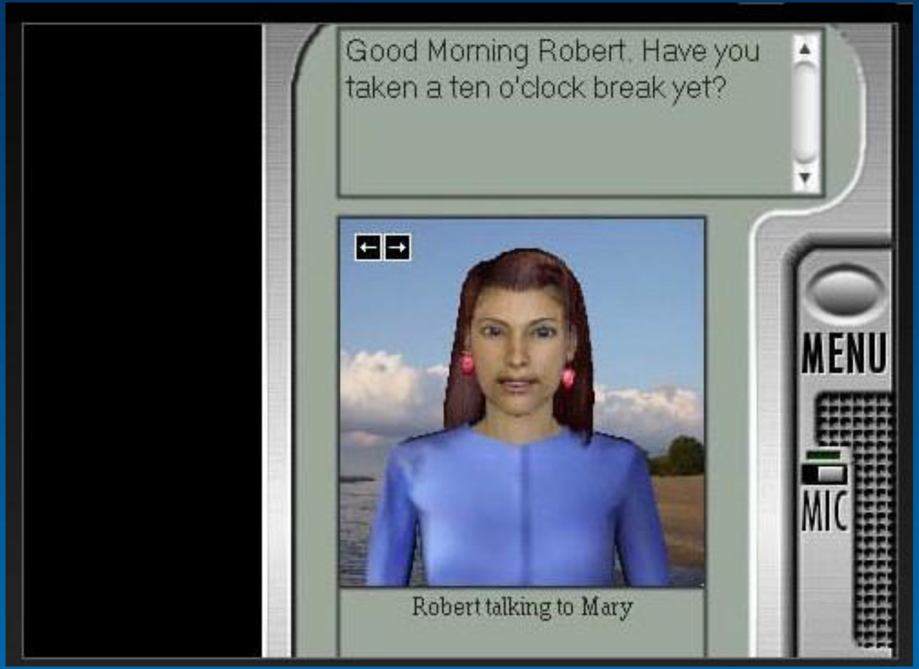
Surgical System



Prosthetic Limbs



Your Digital Secretary



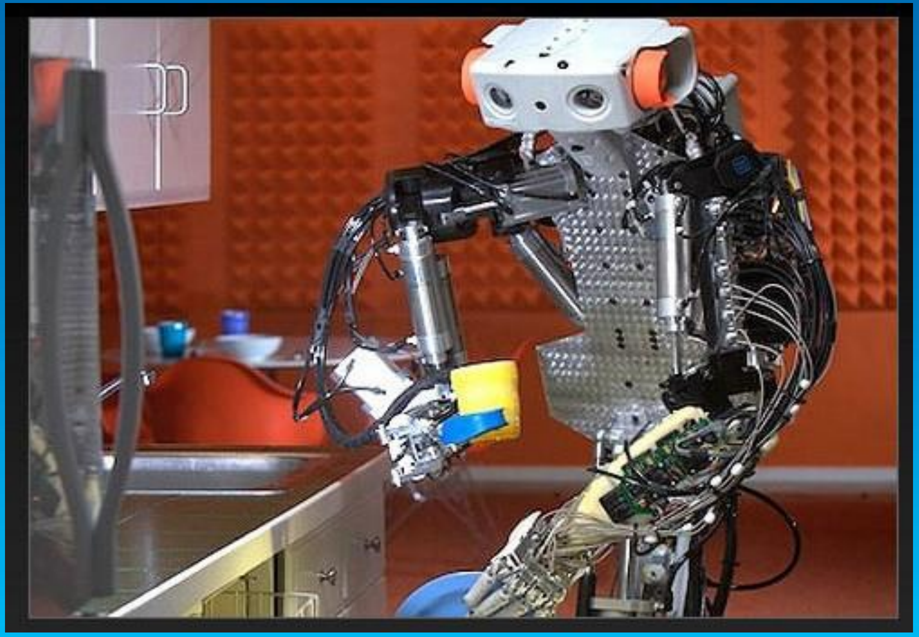
Good Morning Robert. Have you taken a ten o'clock break yet?

Robert talking to Mary

Space Program

All-in-one Floor Cleaner

Walk Like a Man



The AI and ML Revolution is Here

Self-driving cars

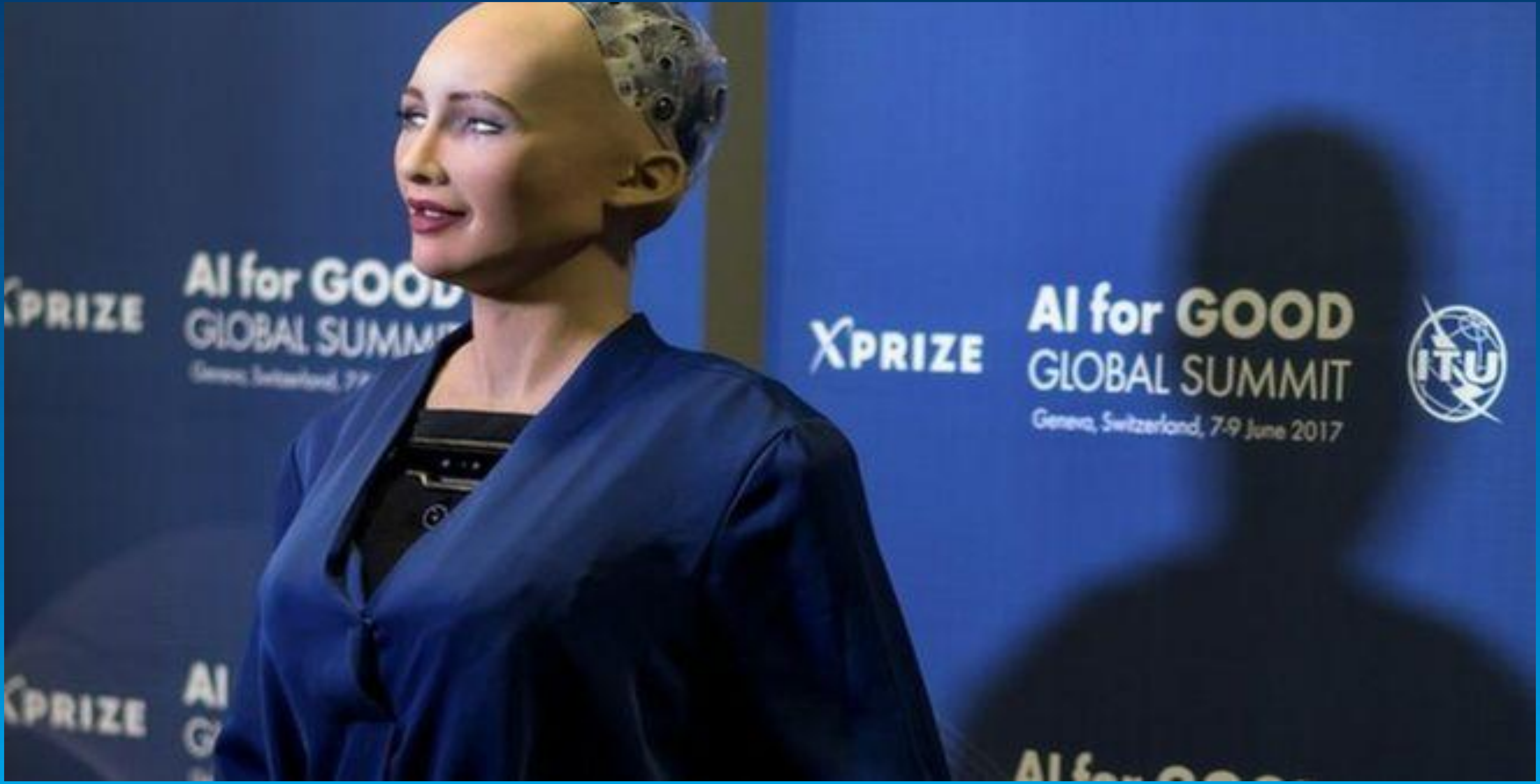
Decision Making: Self Driving (autonomous) vehicles

DISRUPTING – AUTO,TRANSPORTATION, PARKING, CITY PLANING

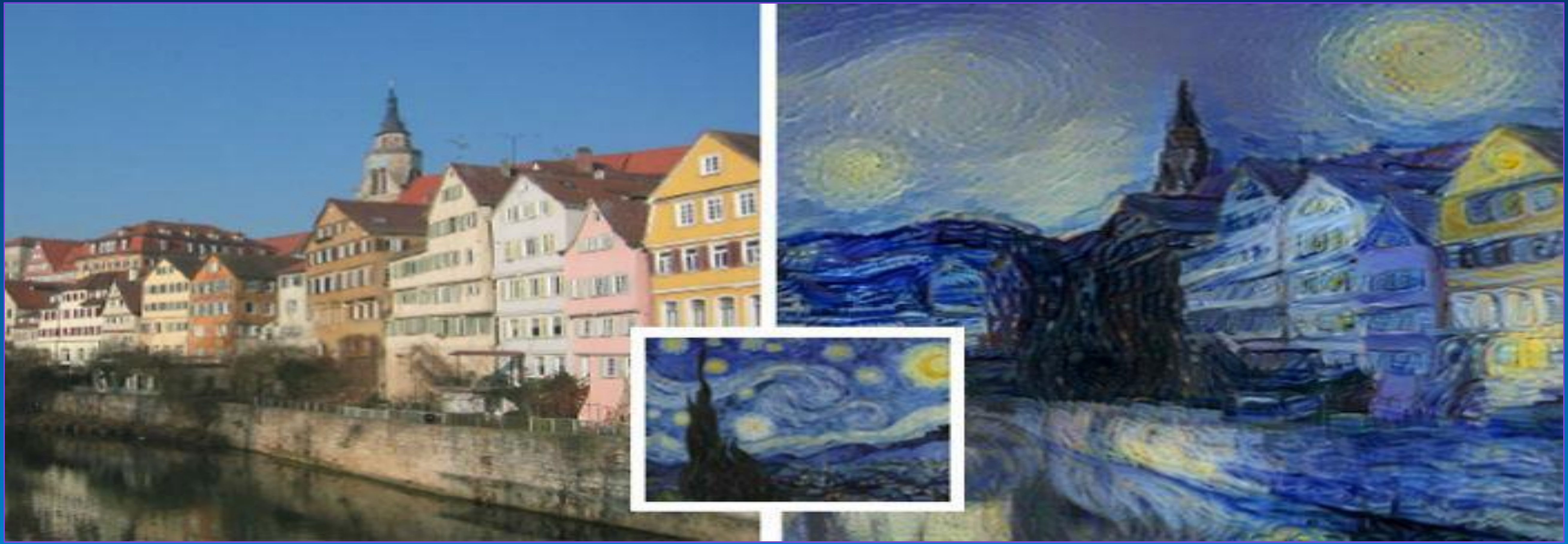
Junior, a robotic Volkswagen Passat, in a parking lot at Stanford University

24 October 2009, By: Steve Jurvetson https://en.wikipedia.org/wiki/File:Hands-free_Driving.jpg

The AI and ML Revolution is Here



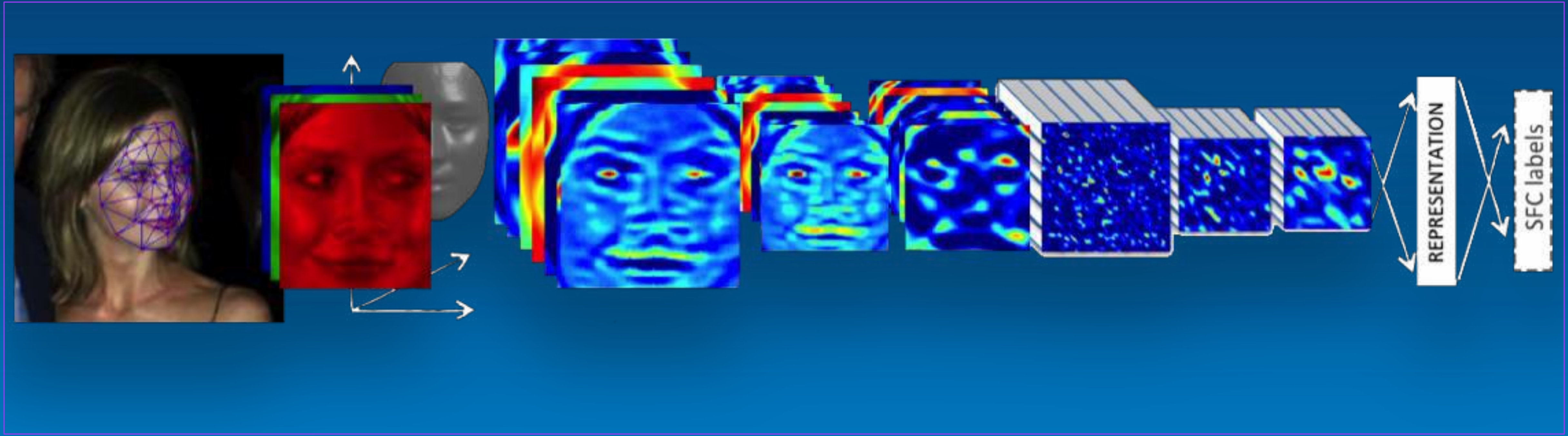
The AI and ML Revolution is Here



AI-generated art

L. Gatys, A.S. Ecker and M. Bethge, A Neural Algorithm of Artistic Style
https://arxiv.org/pdf/1508.06576v1.pdf

The AI and ML Revolution is Here



Computational perception – face recognition (and speech, text, social, video, etc.)

https://research.fb.com/wp-content/uploads/2016/11/deepface-closing-the-gap-to-human-level-performance-in-face-verification.pdf

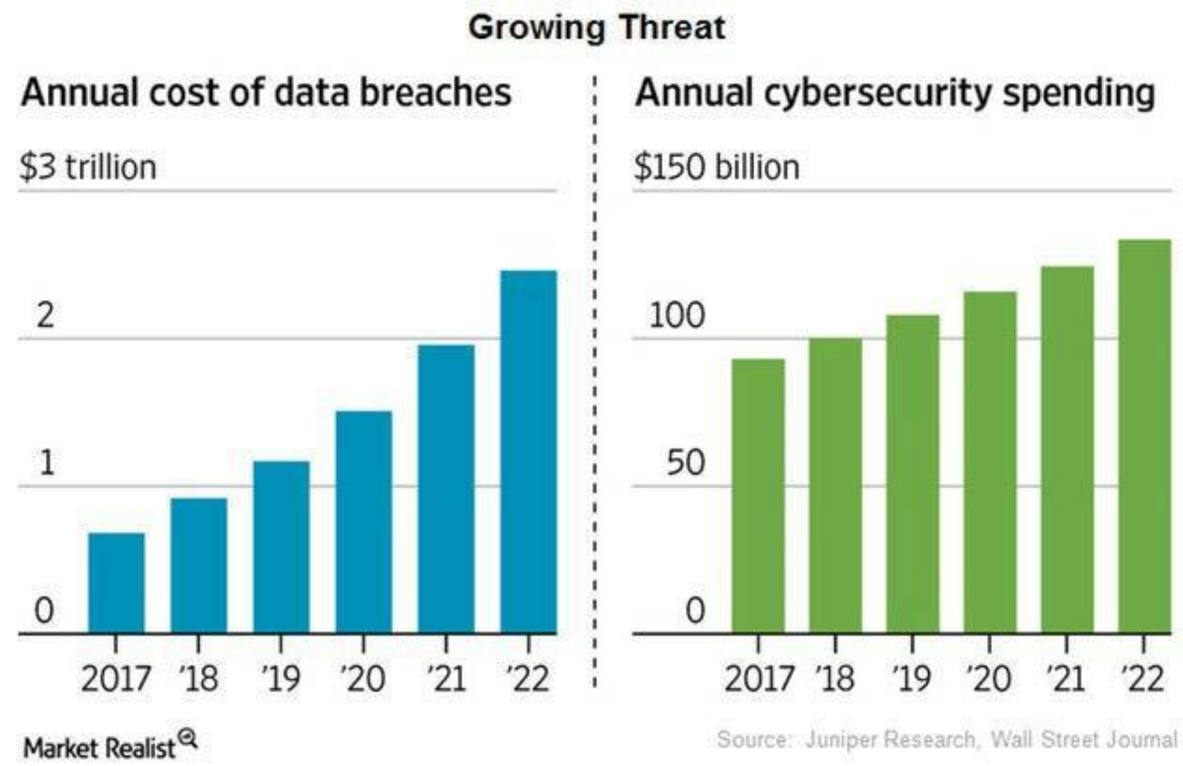
The Current Cyber Landscape Favors Malicious Actors

Global information solutions company, Equifax, has reported a major cybersecurity incident affecting 143 million consumers in the US.

Anthem: Hacked Database Included **78.8 Million People**

”Big Four” accounting firm **Deloitte** was likely **breached** in **October or November 2016**, but wasn’t **discovered** by the firm until **March 2017**

SEC reveals it was hacked, **information** may have been **used** for **illegal stock trades**



Source: Juniper Research, Wall Street Journal

The Cost of Cyber Security Operations Continues to Increase without Mitigating Risk

Most cybersecurity Attacks today are automated, from AI-powered Distributed Denial of Service (DDOS) attacks to phishing scams and ransomware.

The Increased Threat Landscape

- **$1 billion**: Cost of ransomware attacks alone last year
- **$158**: Average global cost of data breach per lost or stolen record
- **25%** of large organizations experience recurring incidents
- **229 days**: the average time to identify a malicious attack

You Can’t Afford To Stay Stagnant:

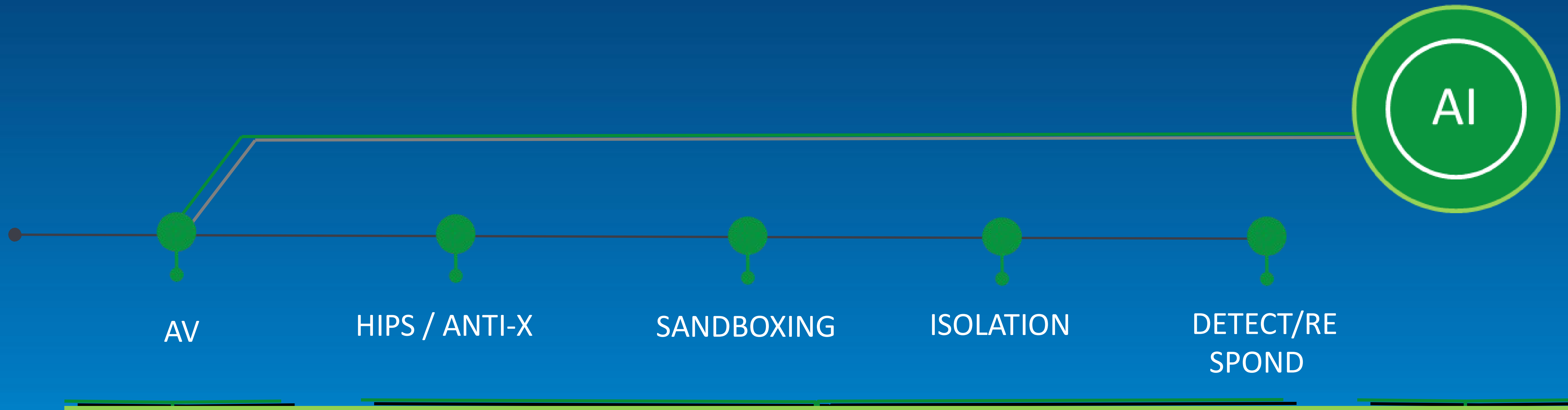
- In 2004, the global cybersecurity market was worth $3.5 billion — and in 2018 we expect it to be worth more than $150 billion.
- Global cybersecurity spending will exceed $1 trillion from 2017 to 2021
- The cybersecurity market grew by roughly 35 X over 13 years.
- We anticipate 12-15 % Y-o -Y cybersecurity market growth through 2021, compared to the 8-10 % projected over the next five years.

The Future of Security

Past

Present

Future



P

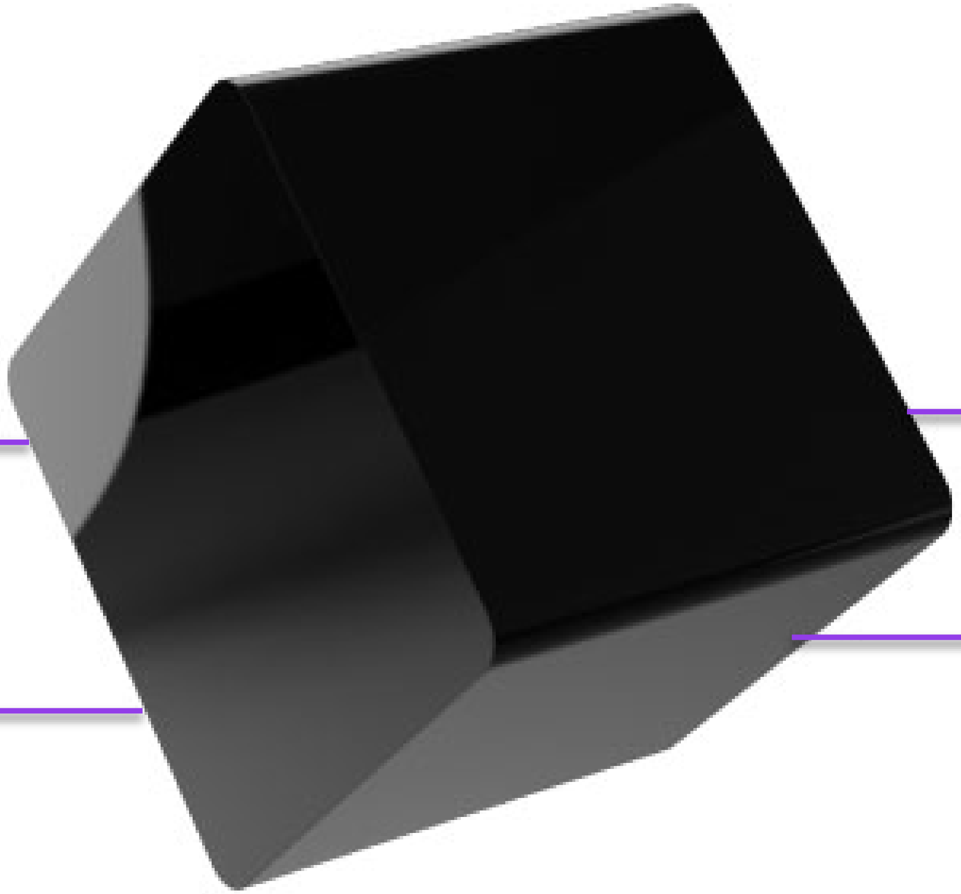
Hu

n

Threat actors could also employ AI tools to discover new vulnerabilities and design exploits and other attacks, in a fraction of the time it's taking them now.

AI could be used as an effective tool to help them decide what, who and when to attack.

Looking into the heart of AI’s Dark Secret



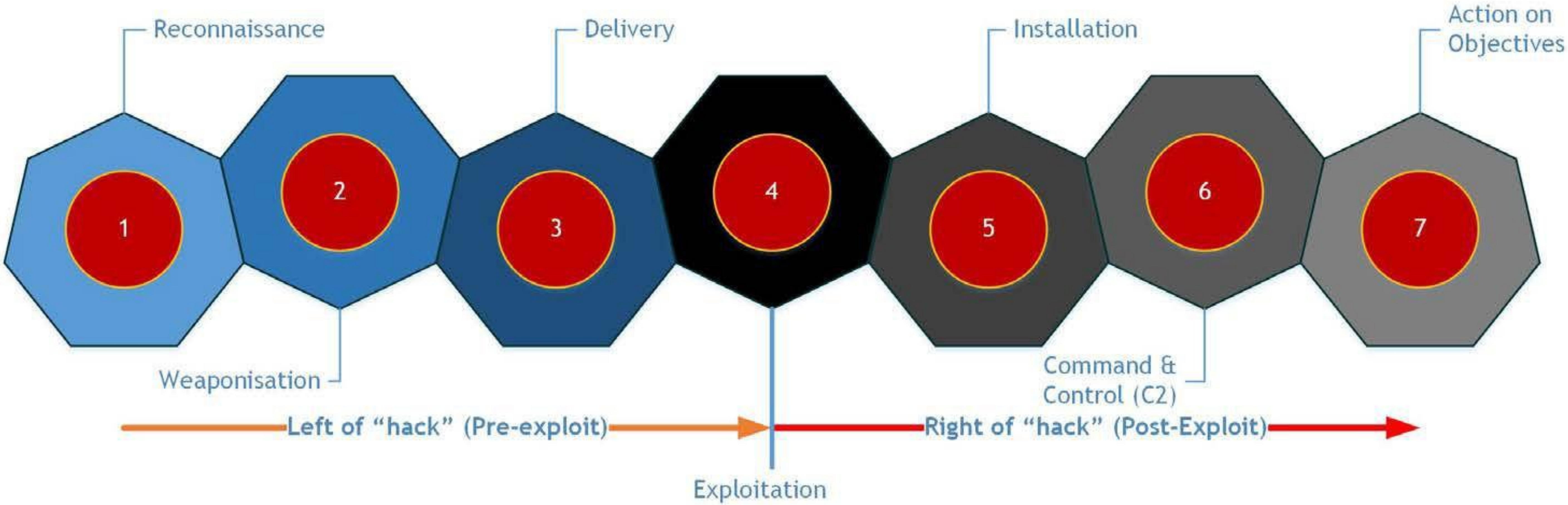
What’s inside the box?

Self modifying algorithms – who to interrogate?

Are we willing to let machines make decisions we don’t understand?

Algorithmic regulation – where and how?

AI fighting Cybercrime



Applications of AI in Cyber Security

- Intrusion detection
- Examples
  - Malicious JavaScript and other scripts
  - Malicious Non-Executable Files
  - Malicious Executable Files
- Inappropriate Web and Email Content
- Phishing
  - Derive probabilistic models of phishing attacks
  - Derive probabilistic reputation models for URLs

AI Changes the Deployment Game

- Make Security Simple

- AI not only improves efficacy, it also changes the deployment model and makes cybersecurity implementation and operation a seamless, smooth process.

- Because of the advanced features of ML, you no longer employ traditional AV technology and tactics, including:
  - Incremental storage
  - Scanning machines
  - Re-imaging machines

- You can remove large endpoint agents that create performanc friction for enterprise users.

AI and Machine Learning Helps You:

- Use minimal system resources (1-2% CPU usage and 40-50 MB of memory)
- Prevent attacks with superior speed (in milliseconds)
- Replace ineffective traditional AV tools (or augment existing security)
- Achieve efficacy rates of greater than 99% (compared to 50-60% with antiquated signature-based AV)

AI / ML Adoption

Drivers

- Scaling and velocity
  - Humans are slow
  - Humans are
  - expensive Data
  - growth
- Automation
  - Threats evolve. Do you?
- Sophistication
  - Complex threats
- 360-degree protection
  - Firewalls talking to email servers and endpoints

Benefits

- Automated protection
- Faster response and protection
- Personalization
  - Learn to adapt to me, unobtrusively
- Usability

Doing AI & ML (Correctly) is Hard!

BOUNTIFUL DATA

- 9 Trillion rows of security data
- 4.5B queries processed daily from 175M endpoint devices
- 2B emails scanned daily
- 1B previously unseen web requests scanned daily
- Outputs from other systems & products

LEADING EXPERTS

- Dedicated org of recognized machine learning experts
- Experts - attack investigation team
- Centuries of combined ML experience

ADVANCED TECHNIQUES

- Ensembling
- Boosting
- Sequential Learning
- Deep Learning
- Automation at Scale

FEATURES / DIMENSIONS

- Static attributes
- Dynamic behaviors
- Reputation
- Relations
- Sequential state

The Future of AI & ML in Cybersecurity

- Superpowers for analysts
  - hunting for targeted spearphishing attacks 100x faster
- Threat detection systems that learn to learn
- Real-time conversation monitoring for
  - social engineering, cyberbullying, fake news, help, etc.

The Future of AI & ML in Cybersecurity

Predictive Protection

AI / ML that anticipates attacks and automatically reconfigures for protection.

Fighting an existential threat?

Thanx

Email me at: inderjit.barara@gmail.com

Reach me on Social Media:

Facebook: Technology Evangeist

LinkedIn: InderBarara

Twitter Handle: @InderBarara

Blog: https://technologyevaneglist.wordpress.com/