Combating Cybersecurity

Threats with AI and Machine Learning

Col Inderjit Singh

CIO ,BCL Secure Premises

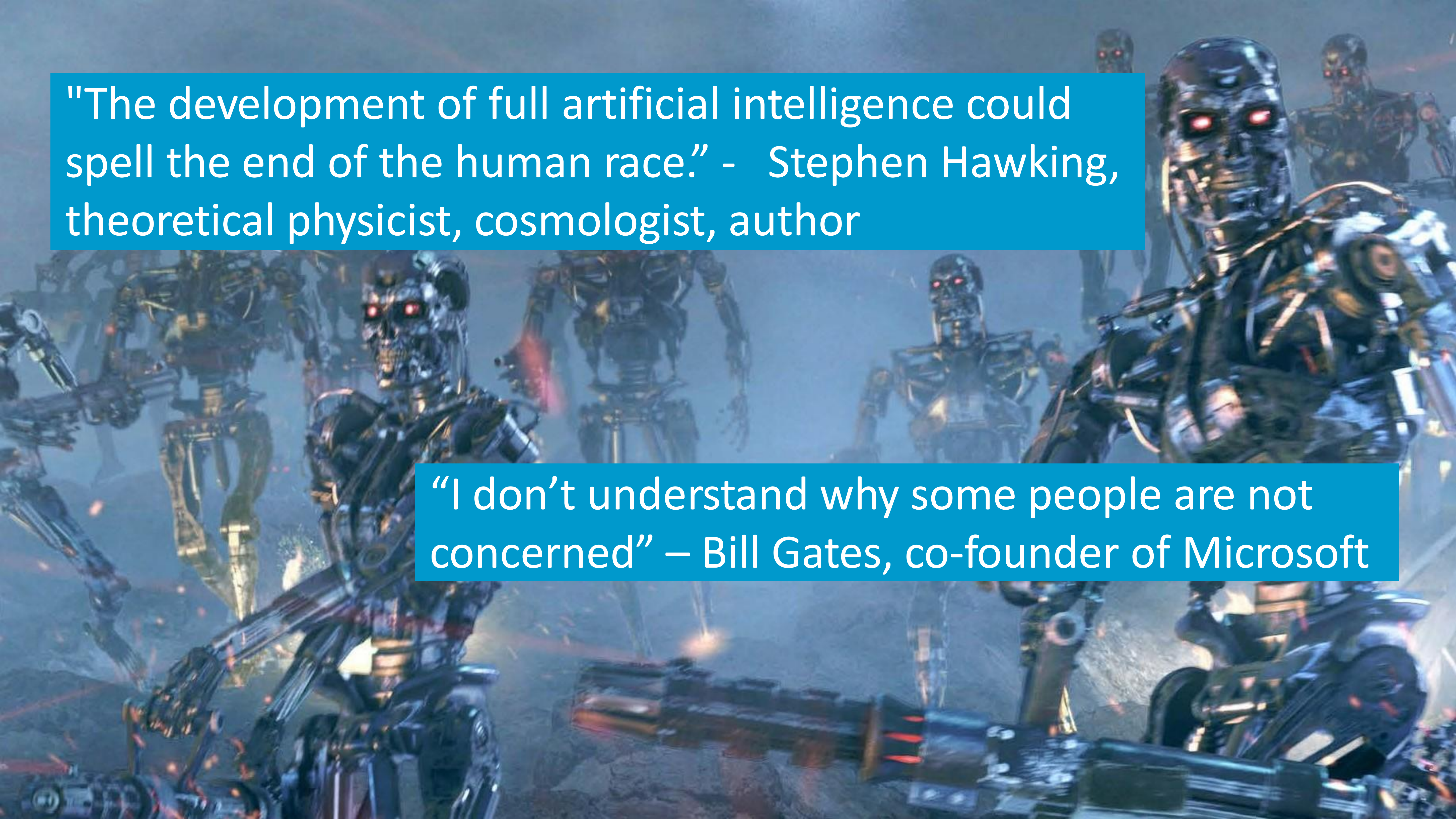
#Whoami

- Alumni of IIT, Kharagpur
- Worked in Defence Forces as Information Security expert for 24 years.
- Over two decades in Cyber Security
- Member of (ISC)2, ISACA, PMI, CCICI
- Council Member CET (I), Fellow IE (I) Fellow IETE (I), Member CSI
- CIO of E-Commerce Company for 2 years.
- Presently, CIO , BCL Secure Premises.
- Founder Member of IESA -IoT Security Forum
- Founder of Cyber Watch India

Contact Me on Social Media:

Facebook: Technology Evangelist
Twitter Handle: @InderBarara

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



"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

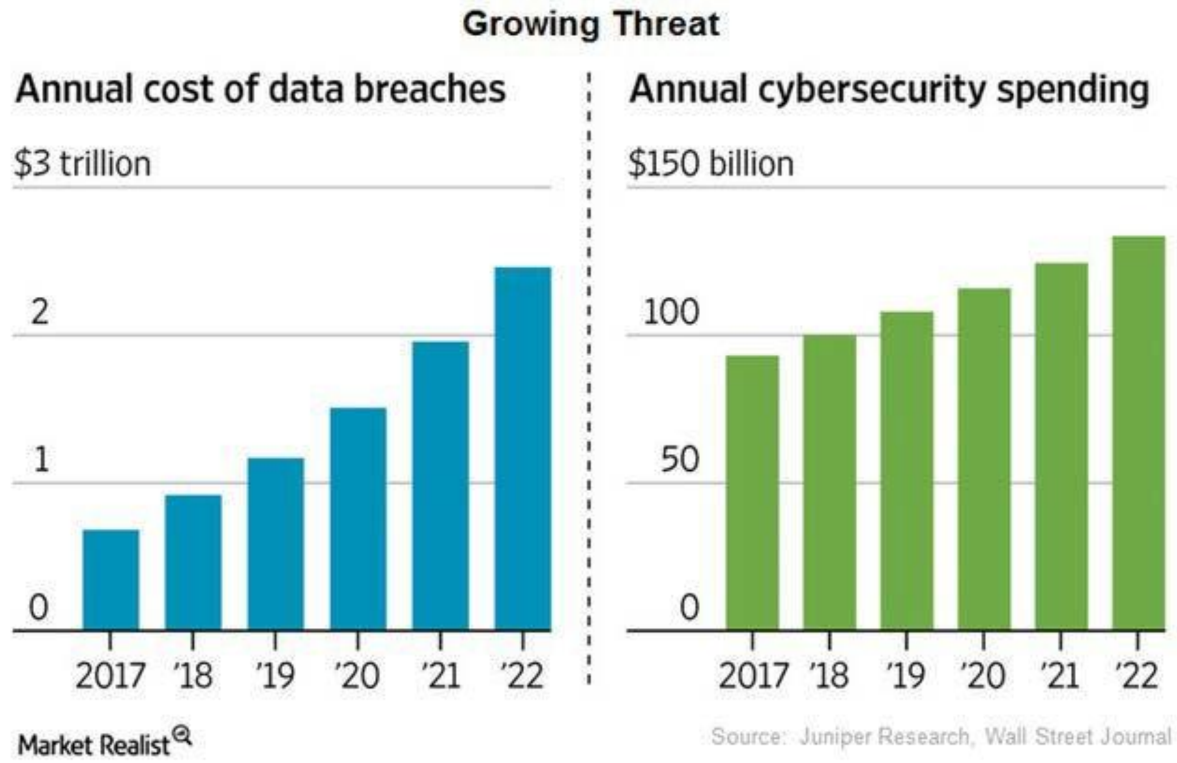
The Current Cyber Landscape Favors Malicious Actors

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

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。

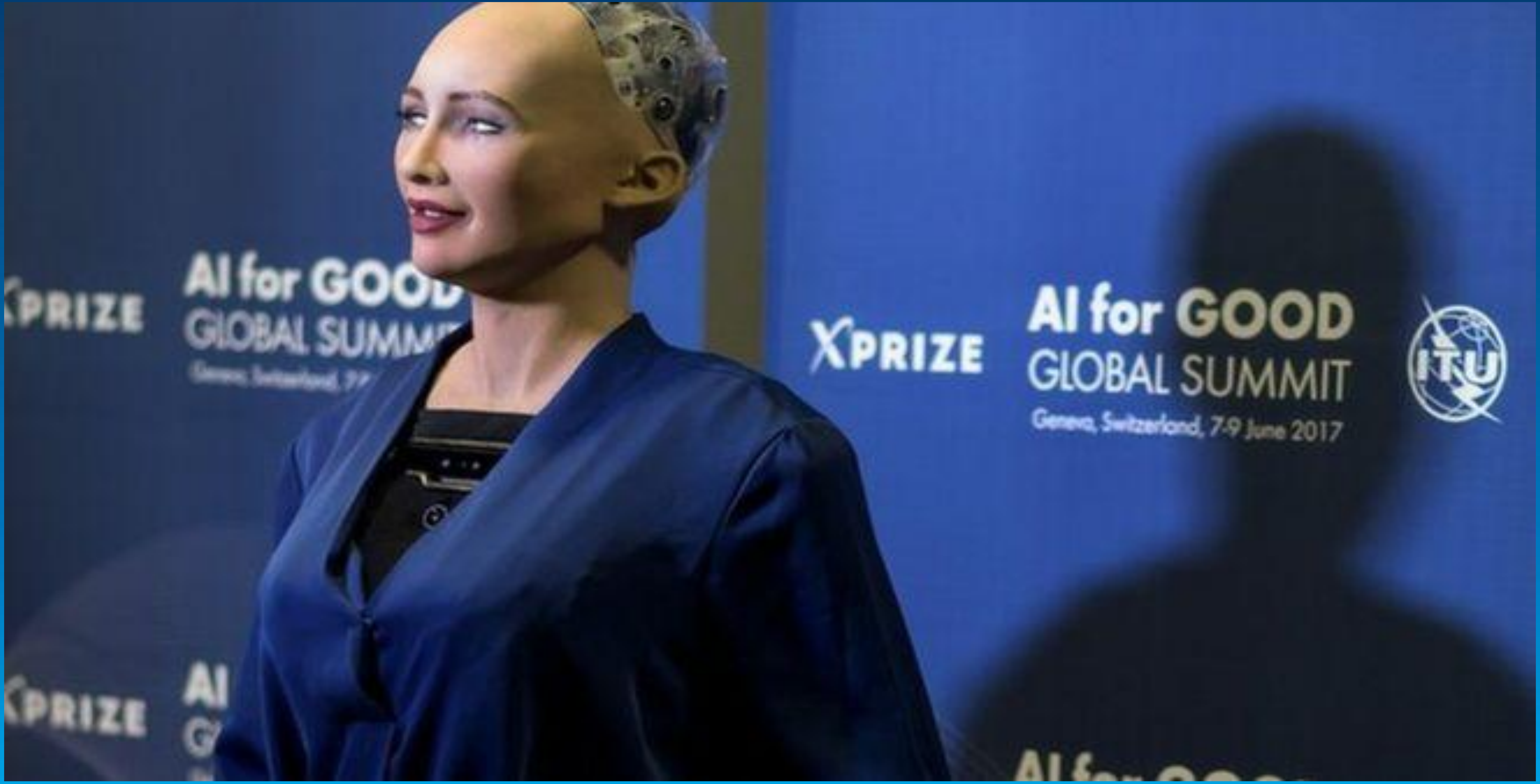
再次，结果并不完美。
他们实际上不少错误。

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

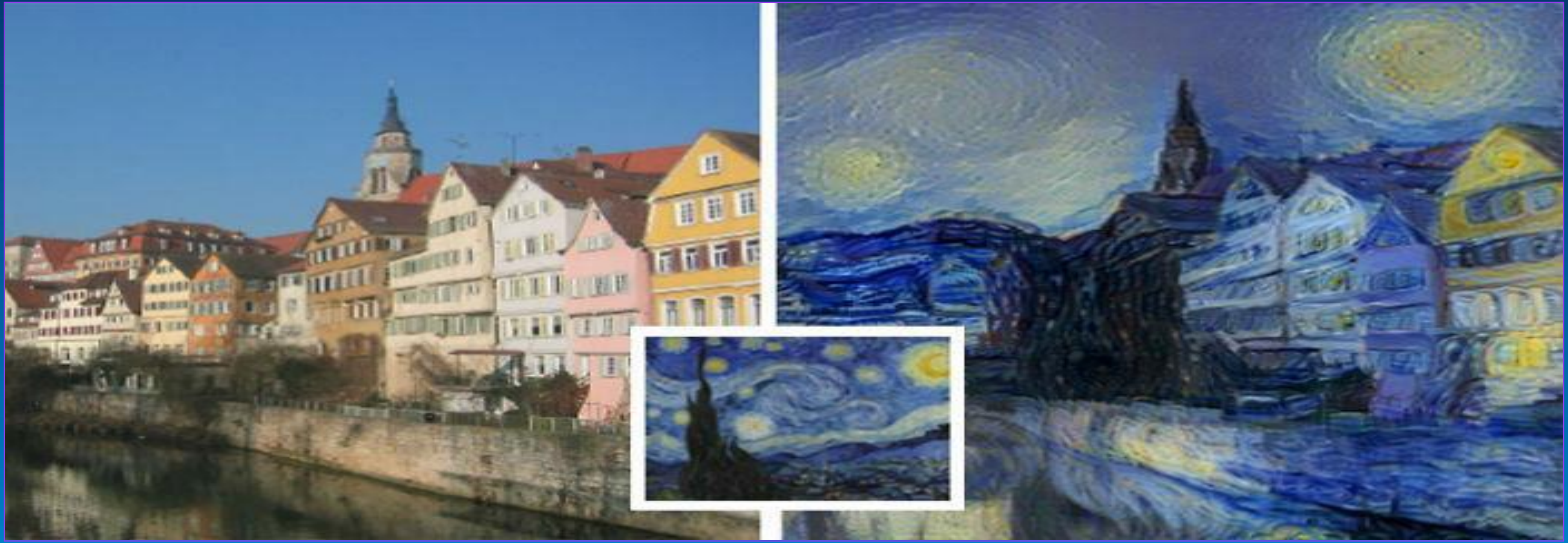
The AI and ML Revolution is Here

Self-driving cars

The AI and ML Revolution is Here



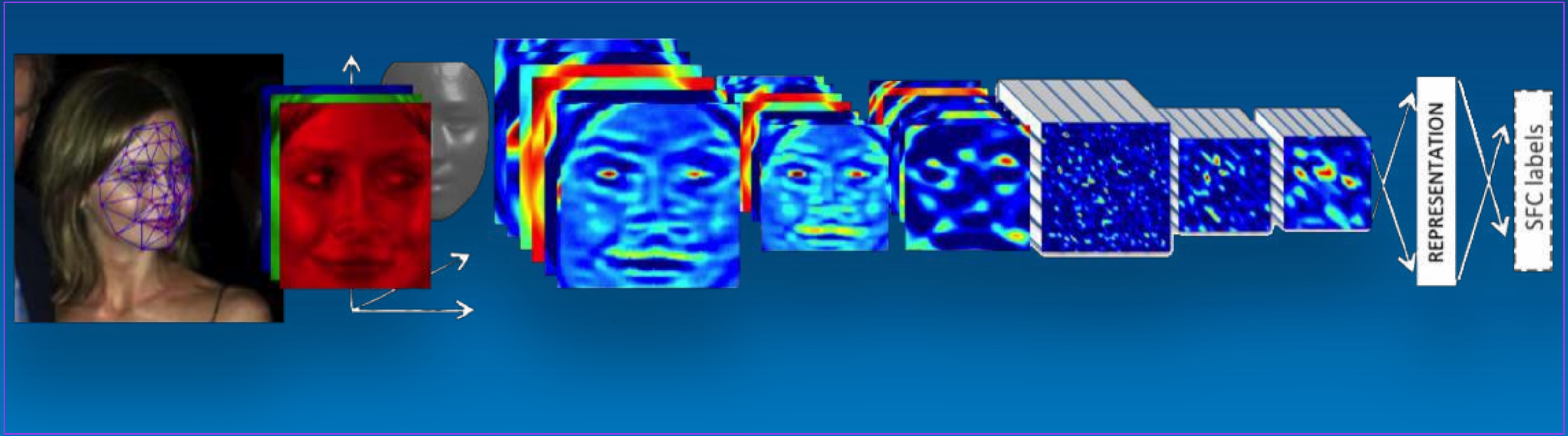
The AI and ML Revolution is Here



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

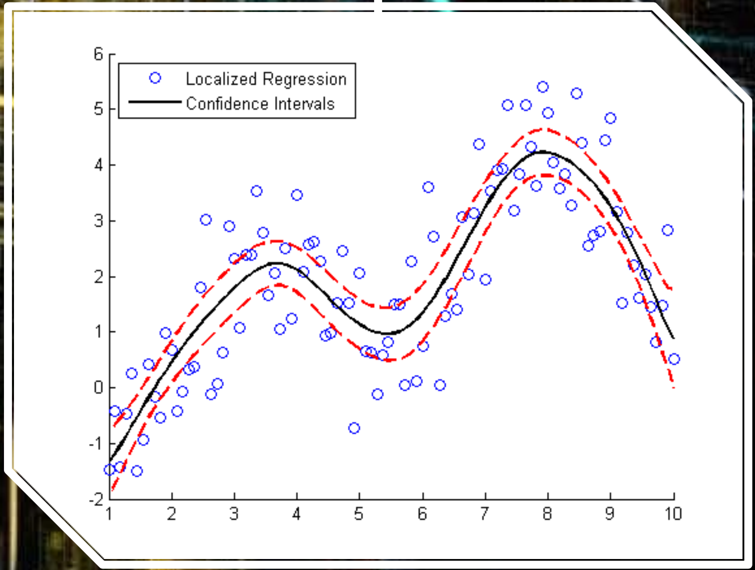


Computational perception – face recognition (and speech, text, social, video, etc.)

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

Artificial Intelligence

Robotic Process Automation



Machine Learning Algorithms

What are ML and AI?

MACHINE LEARNING

The capability of a machine to learn without explicitly being programmed.

learning

ARTIFICIAL INTELLIGENCE

The capability of a machine to imitate intelligent human behavior.

perception

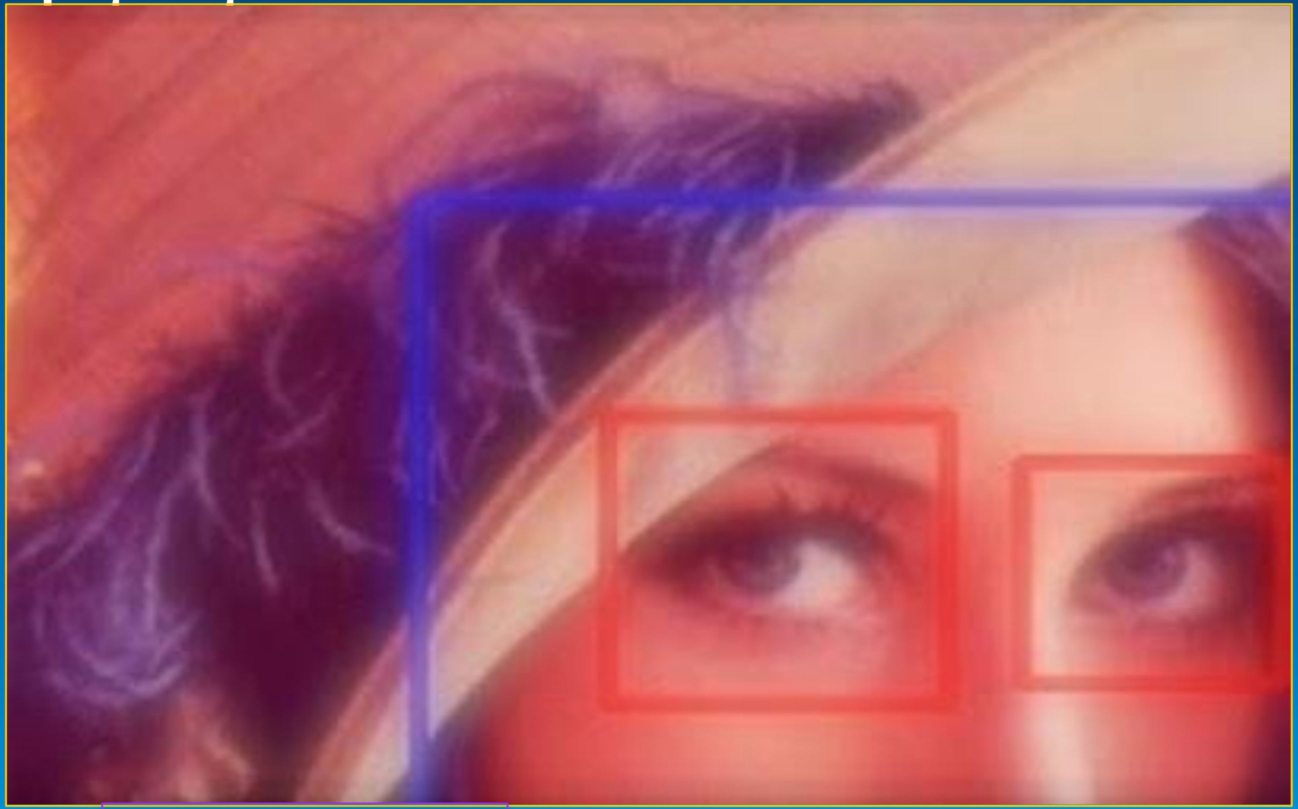
decisions

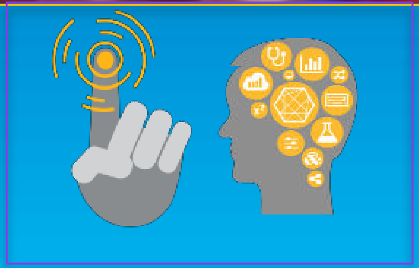
autonomy

An Example: AI vs. ML

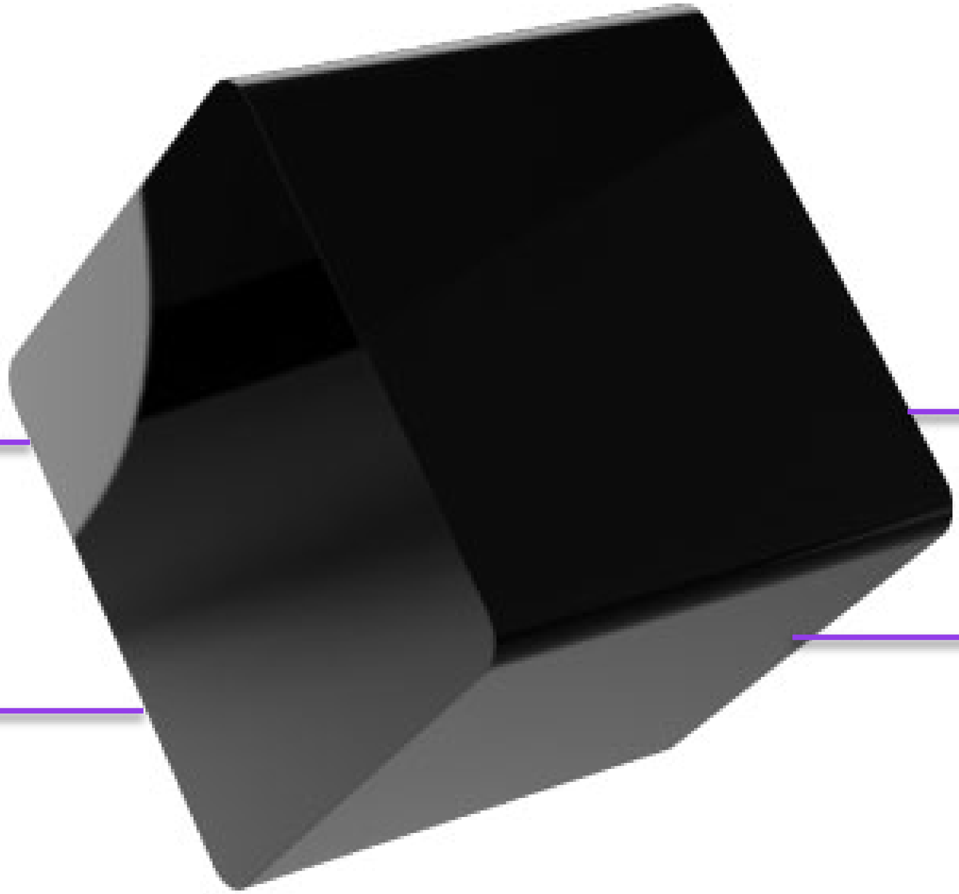
AI: self-driving

ML: pedestrian detection





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?

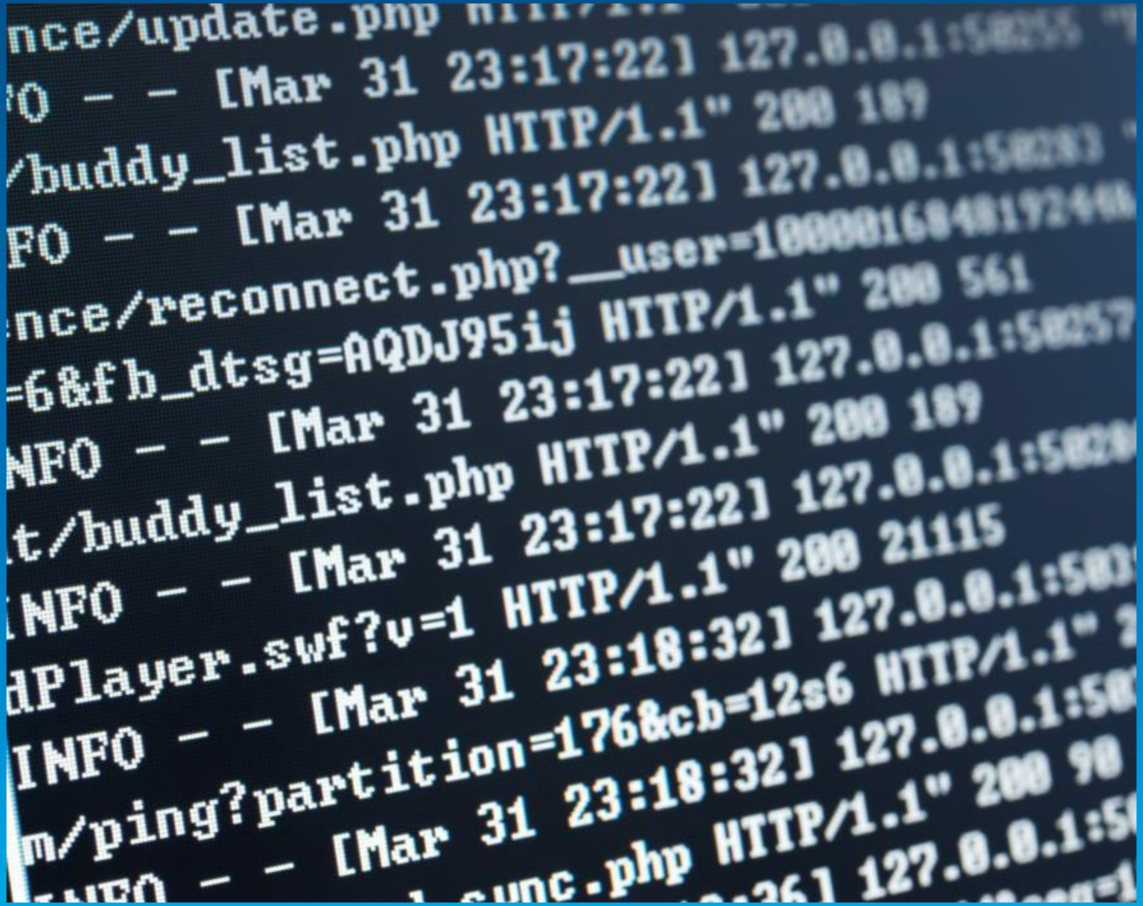
Algorithmic regulation – where and how?

In Cybersecurity We Focus More on Learning

Reasons for ML focus:

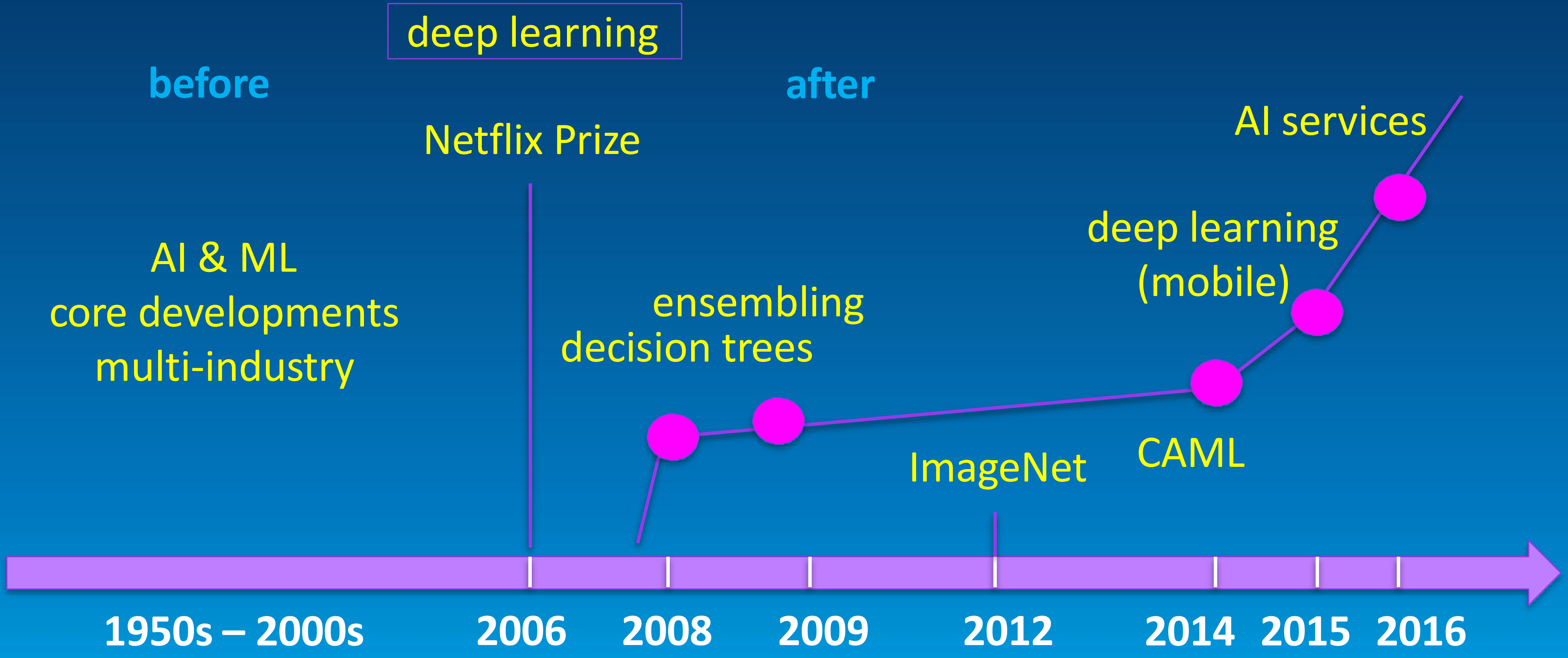
- Complex sequential data
- Not human-intuitive
- What should a program trace or log file look like?
- Scarce | expensive labels
- Closed Research models
- ➔ Slower to advance AI/ML

What should a log file look like?



```
nce/update.php
O - - [Mar 31 23:17:22] 127.0.0.1:50255
/buddy_list.php HTTP/1.1" 200 189
FO - - [Mar 31 23:17:22] 127.0.0.1:50283
nce/reconnect.php?__user=1000016848192
=6&fb_dtsg=AQDJ95ij HTTP/1.1" 200 561
NFO - - [Mar 31 23:17:22] 127.0.0.1:50257
t/buddy_list.php HTTP/1.1" 200 189
INFO - - [Mar 31 23:17:22] 127.0.0.1:5020
dPlayer.swf?v=1 HTTP/1.1" 200 21115
INFO - - [Mar 31 23:18:32] 127.0.0.1:503
m/ping?partition=176&cb=12s6 HTTP/1.1" 2
INFO - - [Mar 31 23:18:32] 127.0.0.1:50
         sync.php HTTP/1.1" 200 90
                  :26] 127.0.0.1:5
```

Is AI/ML New? No*

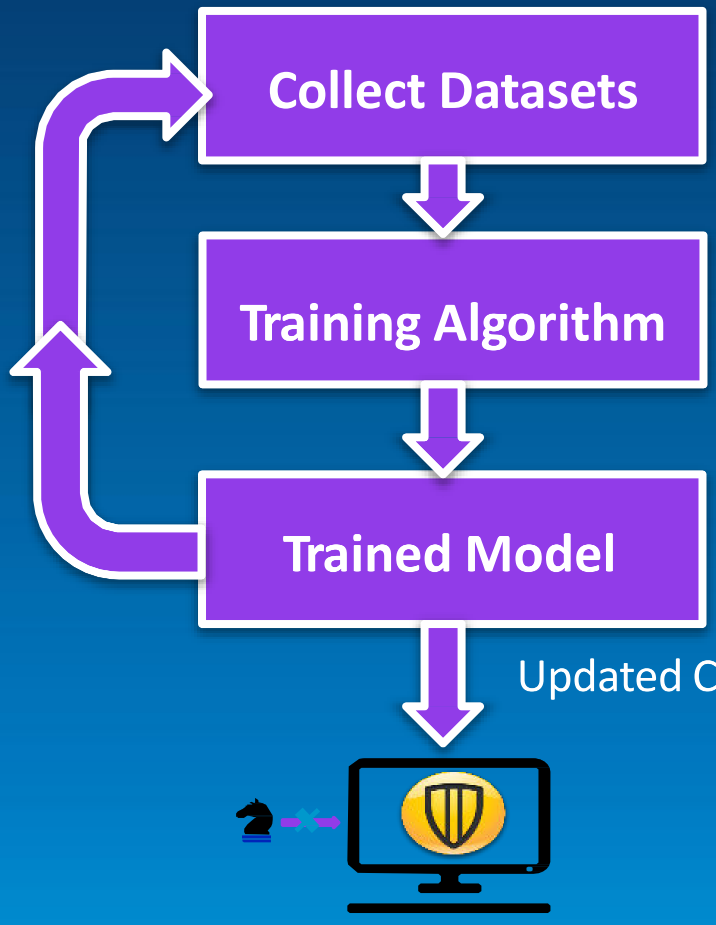


How is AI/ML Used in Security Today?

Yet Another Threat Detector (YATD)

- Straight forward recipe
- Data with labels
- Build / update
- classifiers Debate
- about techniques Rely
  - on data scientists
  - Feature engineering

    Updates & tweaks



Updated Classifiers

Yet Another Threat Detector (YATD)

Researcher/Scientist

How is AI/ML Used in Security Today?

Hidden (Automated) Systems

- Primarily for
- automation Not user-
- facing

Services and applications

- Data + software engineering + ML

Examples:

Continual detector retraining Smart data collection and labeling Anomaly detection for IDS

Why Are AI/ML Important for Cybersecurity?

Malicious Actors and AI

Increasing Success & Falling Costs

Current tools and tactics are already delivering greater success while reducing costs – so any new investment in AI must promise higher returns

High Value Advanced Targets

Target organizations or specific outcomes that were previously deemed too risky of exposure now could potentially become feasible with AI

Individualized Large-scale Compromise

Today centralized targets are prized targets but while they have high yield they become public. AI could allow for large scale decentralized compromises that are hidden

Short time window

When highly prevalent vulnerabilities are announced, some organizations may not respond quickly – AI could allow malicious actors to capitalize on that window of opportunity

Cyber Security Imperatives To Achieve A More Favorable Equilibrium

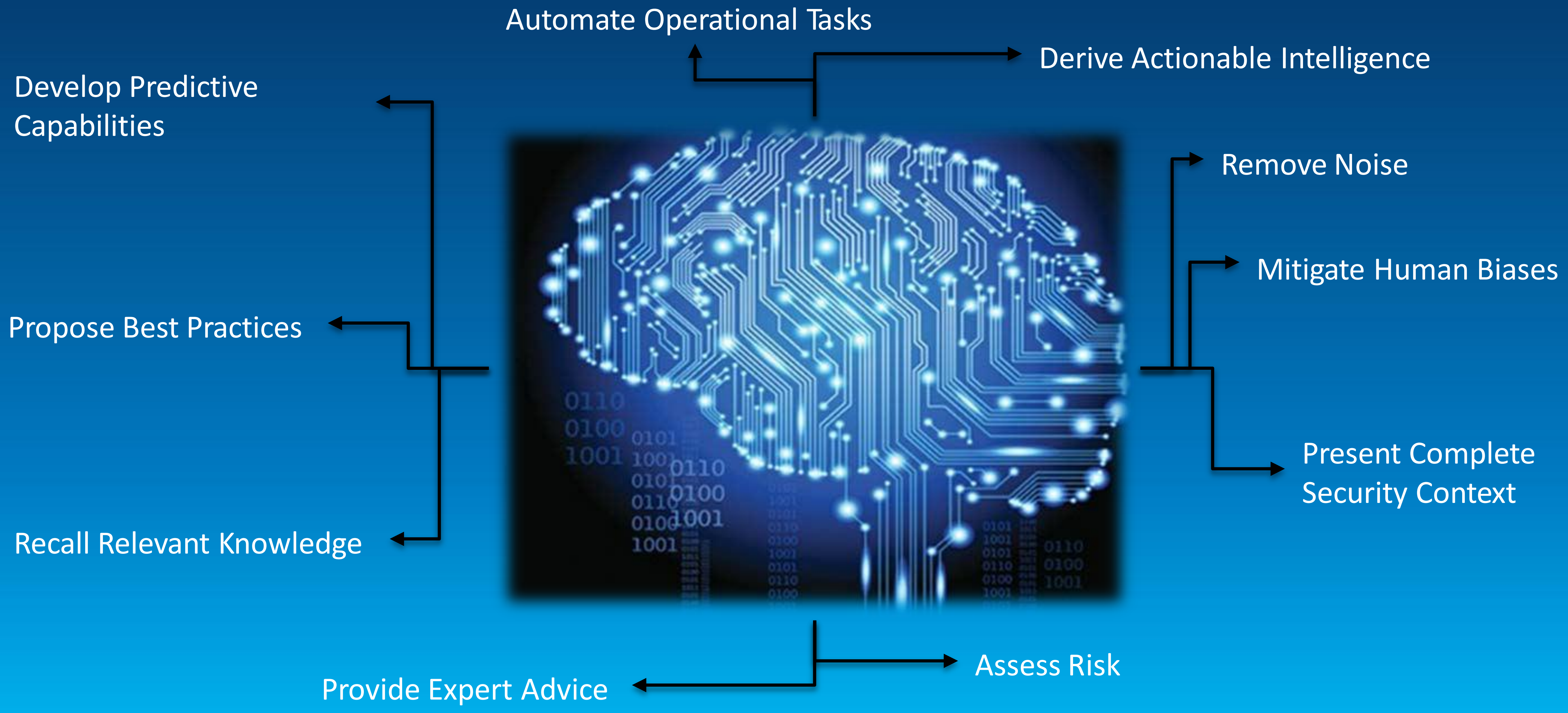
Scale Security Ops With an increasing volume and sophistication of attacks organizations need a force multiplier for their security teams

Assist Decisions Given a broader threat surface area security teams need assistance in effective and accurate data driven decision making

Improve Responsiveness Due to increasing risk of compromise, institutions and individuals will demand faster response to breaches

Be Proactive The goal is to instrument proactive security controls to minimize exposure to emerging threats

The Appeal of AI for Cyber Security



Automate Operational Tasks

Derive Actionable Intelligence

Develop Predictive Capabilities

Remove Noise

Mitigate Human Biases

Propose Best Practices

Present Complete Security Context

Recall Relevant Knowledge

Assess Risk

Provide Expert Advice

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

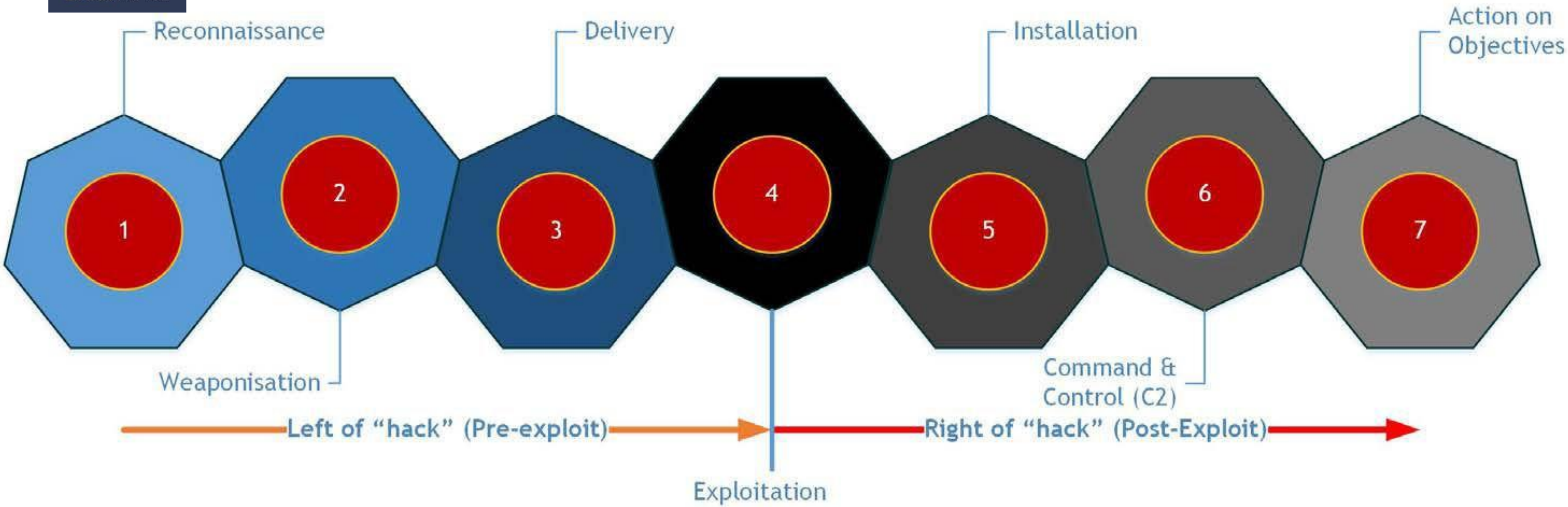
Benefits

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

Fighting an existential threat?

AI fighting Cybercrime

DARKTRACE



observe it

AI Enhanced Kill Chain

Surveillance & Research

- Understanding security controls:
  - Standard practices
  - Specific Target
- Monitoring processes and activities
  - Institutional practices
  - Specific users
- Learn about IT infrastructures and solutions to reveal vulnerabilities

Breach

- Natural Context-aware messaging
  - Email, text, tweets etc
- Adaptive tools
  - Environment-aware behavior modification
  - Evolving malware
- Reputation Spoofing

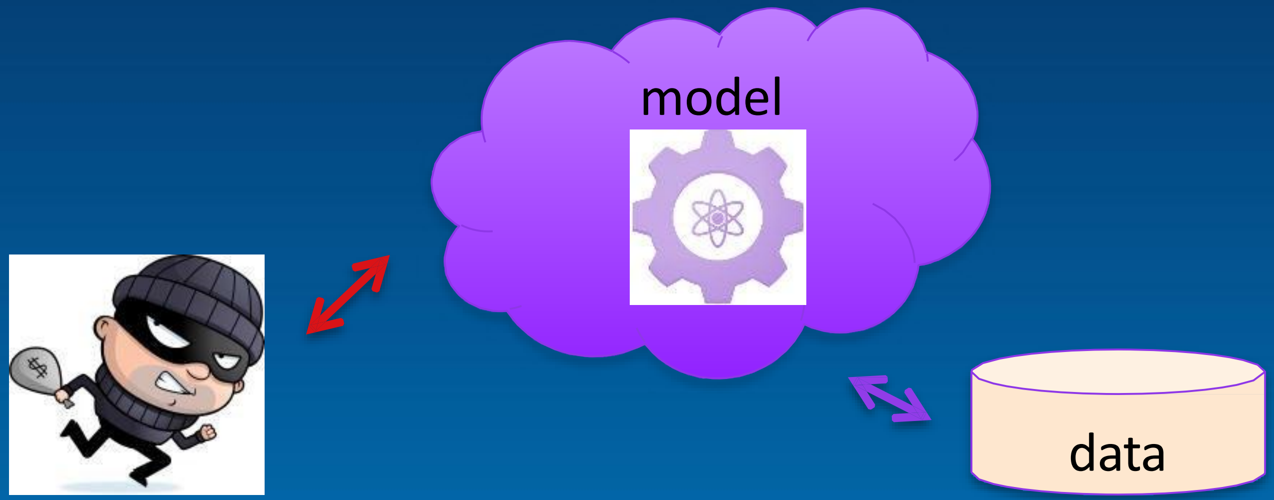
Exploit

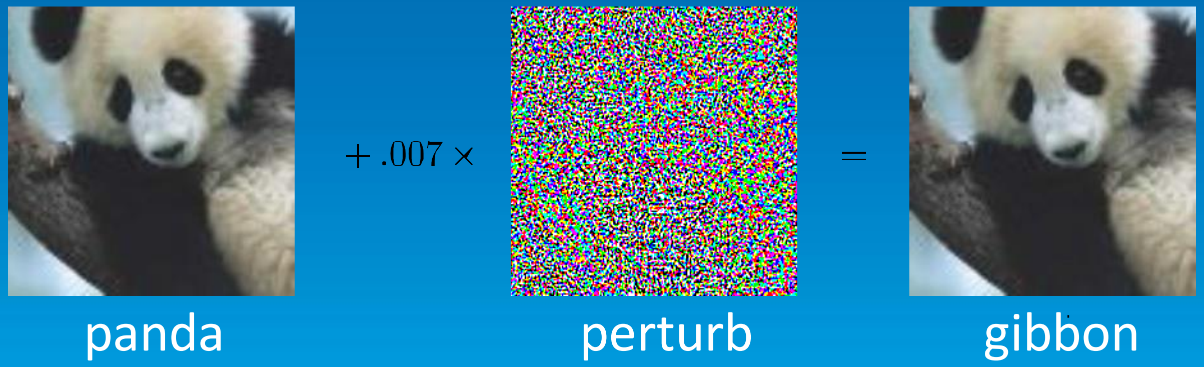
- Diversionary or Evasive Tactics to confuse security controls
  - Generate noise
- Dynamic Tactics
  - Embedded data transfers
  - Entity baseline modification
  - False security event generation

Adversaries Have AI / ML, Too!!

Adversarial Machine Learning

- Model extraction
  - Adversary learns an approximate model using fewest possible queries
- Poisoning
  - Adversary biases machine learning model through interaction
- Adversarial examples
  - Crafting inputs to defeat ML.





Uniqueness of Applied AI in Cyber Operations

Active Adversary

Assume every action taken will be witnessed and an equal or greater effort will be invested to counter it

Data Availability

AI requires high volumes of high quality data to learn. Data silos and varying formats can affect training

Time Value Tradeoff

Given dynamic cyber landscape use cases need to stand the test of time and context or else can negate value

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

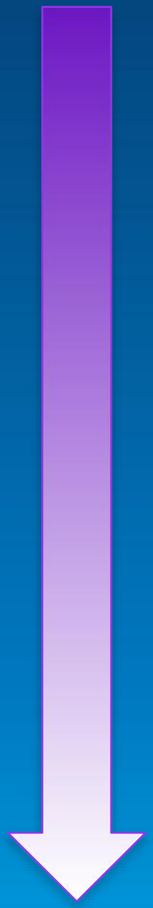
- Ensembling
- Boosting
- Sequential Learning
- Deep Learning
- Automation at Scale

FEATURES / DIMENSIONS

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

The Future of AI & ML in Cybersecurity

now



future

- 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.

Thanx

Email me at: inderjit.barara@gmail.com

Reach me on Social Media:

Facebook: Technology Evangeist
Twitter Handle: @InderBarara
LinkedIn: InderBarara
Blog: https://technologyevaneglist.wordpress.com/