ALION

Thinking in the Box

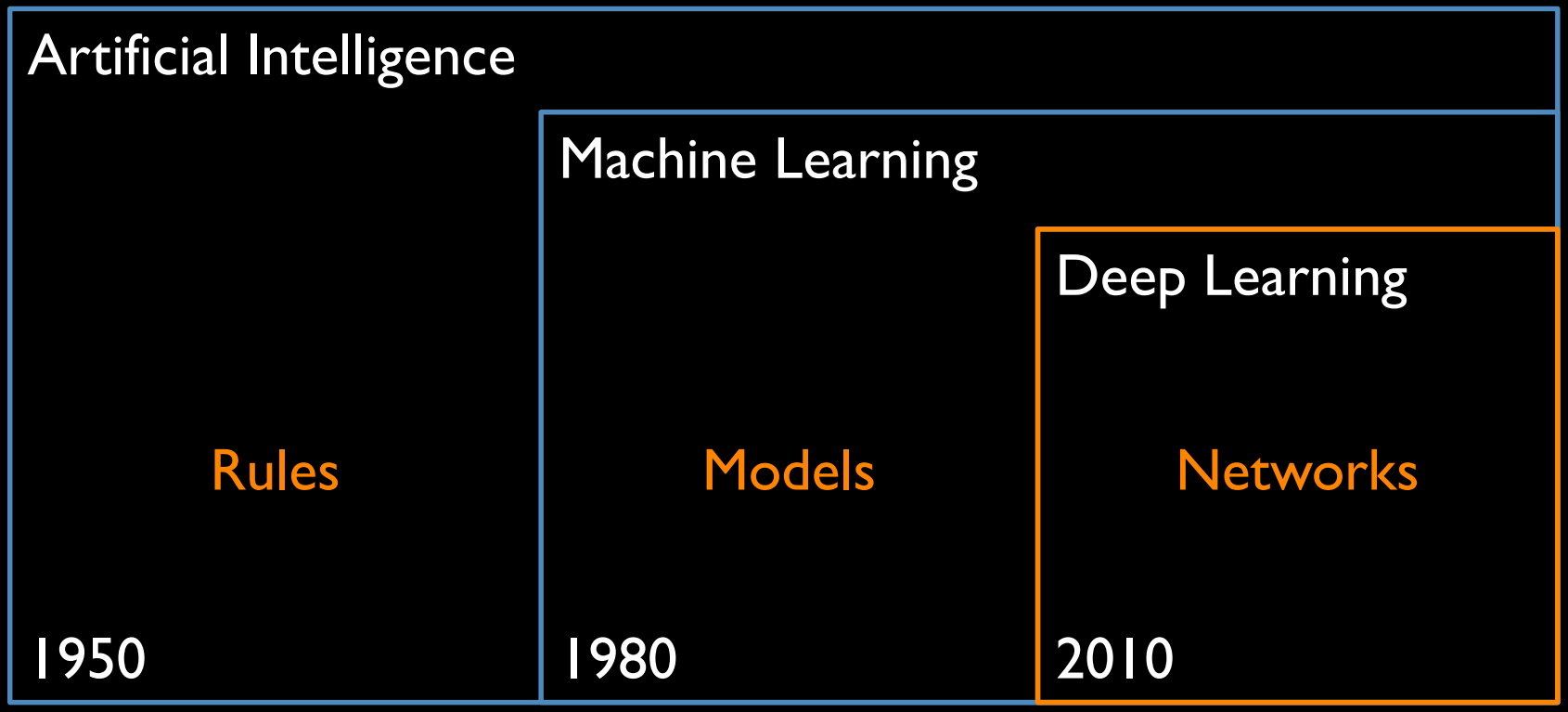
Artificial Intelligence for Cyber T&E

Presented by Turin Pollard, Evelyn Rockwell, and Chris Milroy
Alion Science and Technology

Roadmap

- **What is modern Ai?**
- **Why is cyber so hard?**
- **How can Ai help?**

What? | Eras of Ai



What? | Working Definitions

- **Artificial intelligence (Ai):** doing with computers tasks commonly believed to require intelligence
- **Machine learning (ML):** Ai systems that progressively improve their performance with data
- **Training:** running data through an ML system until it reaches stable and acceptable performance

What? | Machine Learning

- **Core goal: generalize from training data to mission data**
  - Distinct from pure optimization
  - Designed to be executed by machines
- **Many functions**
  - Classification: decision tree
  - Clustering: nearest neighbors
  - Value prediction: regression

What? | Working Definitions

- **Neural network (NN)/artificial neural network (ANN):** an algorithm structure loosely inspired by neurons in the brain

- **Deep neural network (DNN):** a neural network with many layers—at least five, but often tens or hundreds

- **Deep learning (DL):** ML systems that use DNNs

What? | Deep Learning

- **Machine learning:**
  engineered features, learned parameters

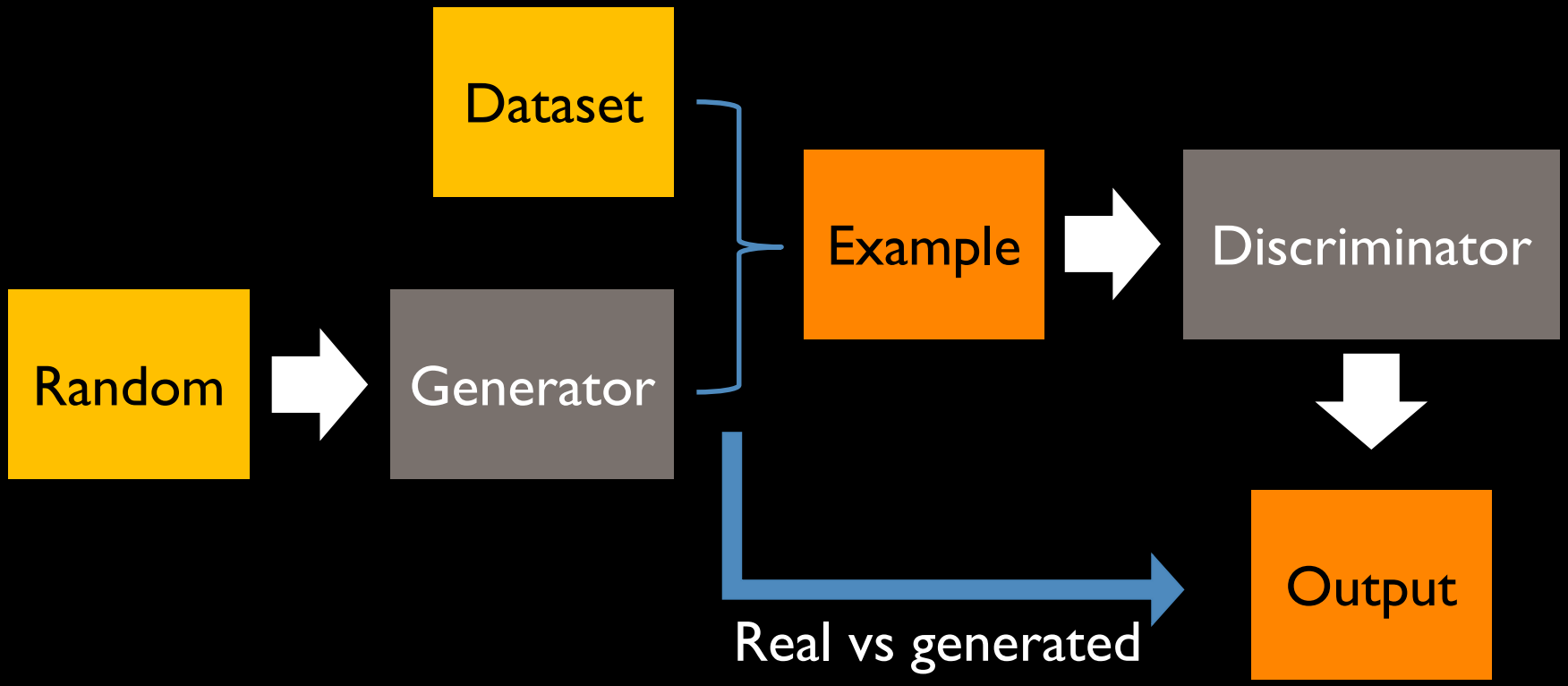
- **Deep learning:**
  learned features, learned parameters

What? | Generative Adversarial Networks

- **Learns how to create new examples like those in a given dataset**

- **Competing subnetworks**
  - Generator (forger)
  - Discriminator (detective)

What? | Generative Adversarial Networks



What? | Generative Adversarial Networks

Why? | Working with magic

magic

power without explanation

^

guaranteed, human-level

Roadmap

- What is modern Ai?
- Why is cyber so hard?
- How can Ai help?

Why? | Asymmetric

- **An Asymmetric Domain**
  - Favoring the attacker
  - Adversaries willing to test on live systems
- **A rapidly moving target**
  - In an unknown N-Dimensional space
- **Not part of traditional Development Processes**

Why? | Requirements

- Are the requirements sufficient for the mission need?
- Are the requirements sufficient to build the system?
- Are the requirements sufficient to against?
- Does the design meet the requirements?
- What is the level of confidence in the result?

Why? | Requirements

- **What is the cyber requirement?**

Why? | What we do instead

- **Fight the last war**
  - Compromise then fix
  - Signatures based blacklists
- **Compliance based engineering**
- **Red Team Assessment**

Why? | In Search of Sunrise

- **Quantifiable cyber security**
  - Durable and Resilient to unknown attacks
- **Not subject to catastrophic compromise**
- **Asymmetric in favor of the defender/developer**
- **Clearly located in the system life cycle**

Roadmap

- What is modern Ai?
- Why is cyber so hard?
- How can Ai help?

How? | Ai for Cyber T&E

- Are the results actionable?
- Are the results repeatable?
- Do the results provide additional insights, compared to traditional cyber T&E methods?

How? | Automation

- **ML and "shallow" DL bring machine speed**
  - What we do today, only faster
- **Signatures, Profiles, Actors based rule sets**
  - Black list based

How? | Anomaly Detection

- **"Real" Deep Learning**
  - White list based
- **First define what is normal**
- **Second, identify deviations**
  - Without having to explain why

How? | Testing and Evaluation

- **Test systems for "zero day" vulnerabilities**
  - We don't know about
  - We don't have to enumerate
- **Provide actionable results to developers**
  - And vectors to our offensive cyber capabilities

How? | Vignette

- **ML automation of known attacks**
- **GANs to simulate activity**
  - Users and Attackers
- **RNN to monitor Health**
  - Expected system state progressions

How? | Next Steps

- **Bring existing Ai based tools into T&E**
- **Develop T&E Specific tools**
- **Continue improving the development process**

Thank you!

tpollard @ AlionScience.com

215.970.0230