AI & CYBERSECURITY

Opportunità e Rischi Operativi

Machine Learning Data Science Meetup
22 ottobre 2019 - Luiss Enlabs Roma

AI & CYBERSECURITY

L'AI nella Cybersecurity ha un ruolo sempre più importante nella **detection** degli attacchi e nella protezione delle **informazioni sensibili**

AI & CYBERSECURITY

La **complessità** raggiunta dalle attuali piattaforme digitali non consente più di affidarsi esclusivamente ai Malware Analysts umani

AI & CYBERSECURITY

Alcuni degli scenari in cui l'AI è stata applicata con successo nella Cybersecurity:

- **spam** filter
- **network** intrusion detection
- **botnet** detection
- **user** authentication

AI & CYBERSECURITY

Altri scenari emergenti che fanno uso di approcci evoluti:

- **biometrics** authentication (neural networks)
- **0days** threats detection (Hidden Markov Model)
- **fraud** detection (Xgboost)

AI & CYBERSECURITY

I diversi approcci dell'AI utilizzati nella Cybersecurity:

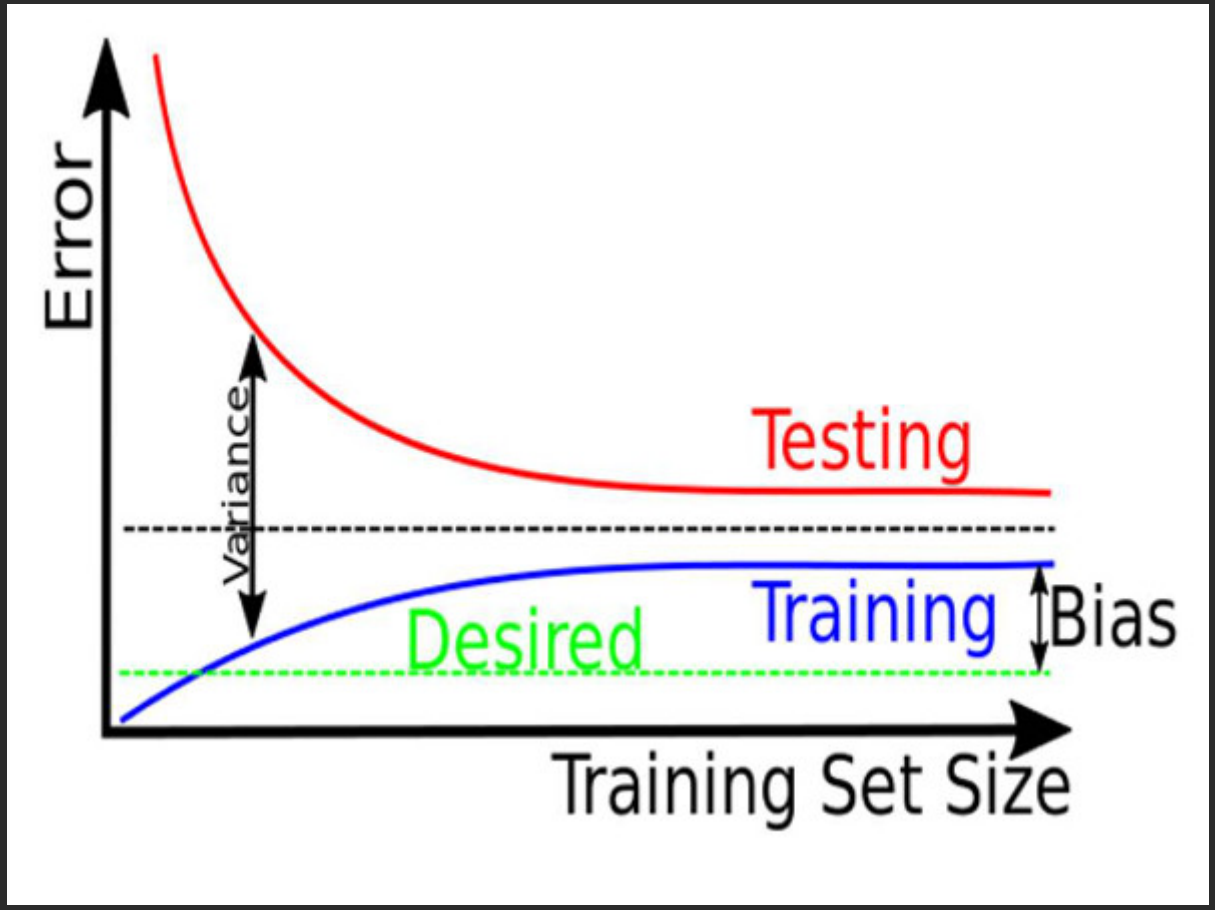
- **supervised** learning
- **unsupervised** learning
- **reinforcement** learning

AI & CYBERSECURITY

Le principali difficoltà operative nell'introduzione dell'AI nella Cybersecurity:

- **biased datasets** (honeypots, malware samples)
- **model overfitting**
- **false positives, false negatives**

BIAS-VARIANCE TRADEOFF



(Image credits: Wikimedia.org)

AI & CYBERSECURITY

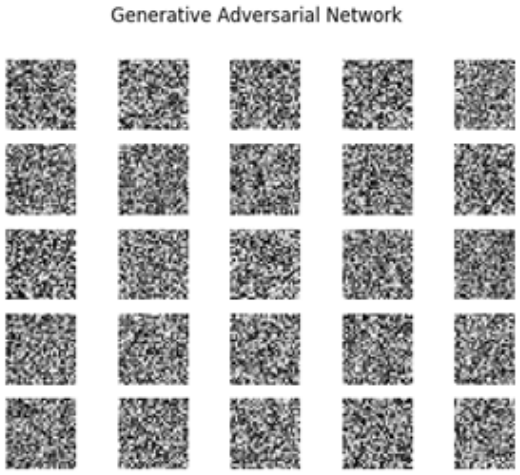
Da tali difficoltà non sono immuni neanche le Neural Networks, anzi:

- **false positives** in facial recognition
- **Adversarial samples attacks**
- **model replication**

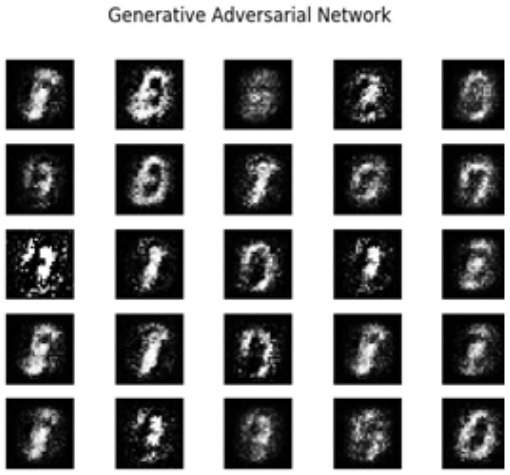
AI & CYBERSECURITY

Tra le minacce emergenti che hanno come obiettivo le procedure di AI possiamo ricordare l'uso delle **Generative Adversarial Networks** (GANs)

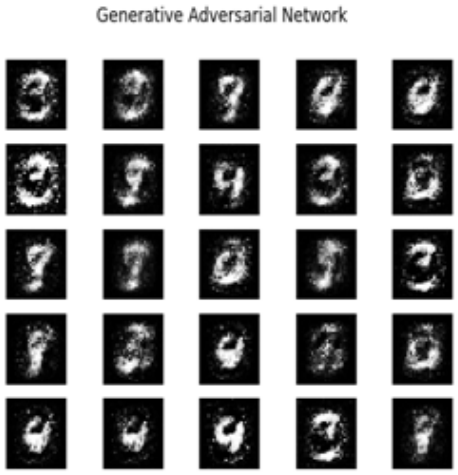
MNIST GAN



0 epochs

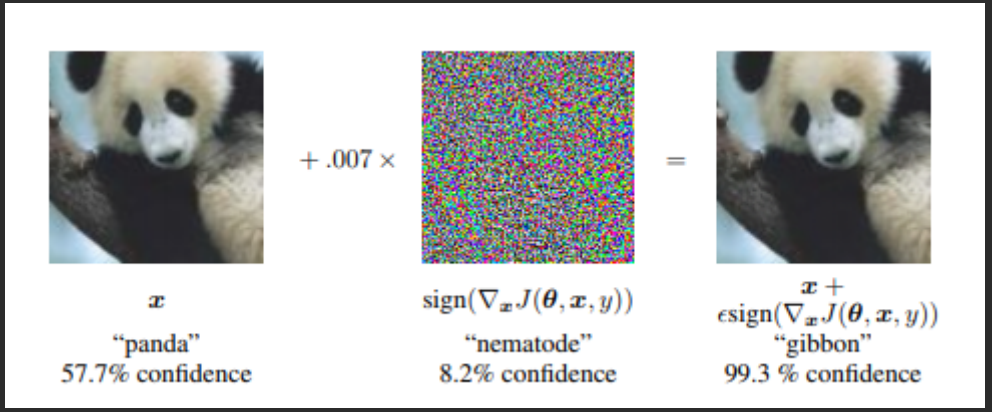


11200 epochs



12800 epochs

GAN IMAGE RECOGNITION ATTACK



(Image credits: "Explaining and Harnessing Adversarial Examples - 1412.6572")

PER SAPERNE DI PIÙ

Hands-on Artificial Intelligence for Cybersecurity